Empirical Evaluation of Information Security Risk Assessment Framework GBM-OA

University of Oulu
Information Processing Science
Faculty of Information Technology and Electrical Engineering
Aleksi Hytönen
12.01.2021

Abstract

Importance of information security is rapidly increasing when new security breaches are continuously reported by companies and organizations. These breaches cause loss of confidentiality, reputation and revenue for companies and organizations. They can also get legal penalties due lack of information security. To improve information security, companies and organizations are required to conduct assessment and audits for their systems to make sure that they do not have open critical vulnerabilities. In addition, information security risks need to be evaluated as part of companies' and organizations' risk management to prepare against possible attackers.

Multiple different information security risk assessment frameworks have been developed to help companies and organizations to conduct information security risk assessment. To find out which framework is suitable for their needs, management needs to compare the different frameworks, estimate how much time and how many people are available for the assessment and how the frameworks have worked previously in the context. In this thesis, suitability of genre-based security risk assessment framework GBM-OA is evaluated in context of centralized CI/CD environment.

A canonical action research was conducted in a team providing centralized CI/CD solution for the company's projects. In the study, information security risk assessment was conducted using GBM-OA, and after the assessment semi-structured interviews were conducted for the participants to find out if the framework was suitable in the context.

The findings show that the framework provided sufficient results for the team without taking much time from the participants. Additionally, participants found value in definition of environment, which helps the team to understand how responsibilities are split to different stakeholders. Downsides were confusing terminology used in the framework and filling of the templates was found compelling. About suitability, it was found that the framework is not suitable in the context as it is. Participants did not like that the assessment should be done separately, but it should be integrated into automation or development cycle. Right now, there is not any instructions regarding integration or iteration, even though it is stated that it is possible. Participants also provided improvement suggestions to add step to the framework for risk impact definition.

Keywords
Information Security, Risk Assessment, DevOps, CI/CD, Framework, GBM-OA

Supervisor
PhD, Professor Tero Päivärinta

Foreword

I would like to thank my thesis supervisor Tero Päivärinta for giving me guidance during my work for this thesis. I would also like to thank him for interesting conversations about the subjects related to this thesis, which helped me wider my mindset about information security, and they gave me new ideas to write about. I would also like to thank the department of information processing science for giving me an opportunity to study a field that I have found very interesting during my studies.

I would like to thank my employer for flexibility and allowing me to use work time to write the thesis. This has provided additional motivation to work on this thesis. In addition, I would like to thank him for asking about the progress of the thesis and making sure, that I am moving forward. I would like to thank my colleagues for participating in the study conducted in this thesis and supporting me with the work. Healthy working environment has made writing of this thesis feel light.

I would also like to thank my significant other for sharing the struggles of writing master's thesis with me. Without her support I do not think that I would had made it to the finish line. I would also like to thank my family for showing interest in my thesis even though they do not understand anything about the field.

Aleksi Hytönen

Oulu, January 12, 2021

Abbreviations

GBM-OA	Genre-Based method combined with OCTAVE Allegro
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation
CI/CD	Continuous Integration / Continuous Delivery
CIRA	Conflicting Incentives Risk Analysis
UP	Unified Process
UML	Unified Modelling Language
ISO	International Organization for Standardization
XML	Extensible Markup Language
ISRAM	Information Security Risk Analysis Method
ISGcloud	Information Security Governance Framework for Cloud Environment
COBIT	Control Objectives of Information and related Technologies
QUIRC	Quantitative Risk and Impact assessment framework
SO	Security Objective
SQL	Structured Query Language
NVD	National Vulnerability Database
CVSS	Common Vulnerability Scoring System
RQ	Research Question
CAR	Canonical Action Research
TC	Target Company
TS	Target Service
AWS	Amazon Web Service
OA	OCTAVE Allegro
PUI	Producers and Users of Information

Contents

List of figures

List of tables

1. Introduction

When computers were just coming to the market, companies conducted business without having to rely on information systems. When time passed and new technological discoveries were made, companies and organisations started to use different systems in business-critical areas, giving them competitive advance against competitors. While computing power increased, also did the possibility of security attacks also increased. Hence making information security a major topic for information systems. This development raised the discussion about information security risk management, which consists of risk assessment, development of countermeasures or mitigation activities and monitoring of risks status. This process allows proactive protection of business-critical assets while also saving resources from protection of invaluable assets or wasting resources in mitigation of small or insignificant risks (Shedden et al., 2011).

When internet became widely used and computers were bought by individual consumers, information security was not a big topic and it did not get much attention. When attacks started to occur against companies, vulnerabilities were just fixed, and the risks were not identified or managed. If company identified a threat, a technical solution was implemented to counter it. At the end of 20th century, researchers realized that information security is not a topic that can be handled using technical solutions alone. As a result of this conclusion, economical point of view started to be a major part of information security risk management. This development allowed managers to see security as an investment, because consequences of security attacks were analysed as economical losses (Acquisti et al., 2006).

Organizations' assets are in constant radar of possible attackers which can be seen as multiple different types to threats against the assets. These threats contain risks that can be identified using risk management. To reduce risks and to ensure that assets and organization's confidential information are kept secret, organizations often rely on technology-based solutions. Even though technological solutions are important component in information security, using only those solution is not enough to cover all risks. Bulgurcu et. al. (2010.) argue that even though organizations invest heavily in technological solutions to protect their assets, number of breaches is still increasing. They also argue that to cover all risks, both technological solutions and socio-organizational approaches should be implemented.

In this thesis I talk about information security risk assessment, which is part of risk management. Risk management consists of three parts: (1) risk identification, measurement and assessment, (2) risk evaluation and mitigation, and (3) risk control and monitoring (Xie et al., 2011.). I want to find out what frameworks there are available to conduct risk assessment, how to implement risk assessment framework in practise and how well the selected assessment framework works in the implemented context.

To find out how to implement risk assessment framework in practice and how well the selected framework suits to the context, canonical action research was conducted in a company. In evaluation of the framework, qualitative semi-structured interviews were held with participants of the assessment.

The structure of this thesis is as follows. First, I will discuss about prior research conducted regarding risk assessment frameworks and I want to find out what kind of options there is for risk assessment. This discussion can be found from section 2. Second, I will introduce the context and method used to implement risk assessment framework in practice. This can be found from section 3. Third, I will describe how the implementation was done and what were the outcomes of the implementation. This can be found from section 3.4. Lastly, I will conclude what was done in this thesis and what were the most important findings and learnings. I will also discuss about limitations of this research and what could be the possibilities for future research.

2. Prior research

In this section I will introduce prior research conducted about risk assessment. I will also introduce few frameworks that are developed to conduct structured risk assessment. The objective of this section is to introduce different studies conducted about risk assessment and what different approaches to conduct risk assessment there are available.

2.1 Risks, threats, and vulnerabilities in information security

Risk is usually defined as a combination of the probability of occurrence and its consequence. In information security, risk can be defined as a possibility that a threat will take advantage of vulnerability of an asset or multiple assets, and thereby causing harm to the target of the attack. Risk consists of threat or threats which affect one or more asset, which would have a negative effect to the asset or assets. An example of information security risk would be a hacker exploiting social engineering (threat) to an employee of a company, who does not have much understanding about information security (vulnerability), leading to unauthorized access to company resources (assets) which would cause loss of integrity and confidentiality of sensitive information (consequence). Identification of these risks, development of countermeasures against these risks and monitoring these risks state is called risk management (Gordon and Loeb, 2005).

2.2 Information security risk assessment

Information is an important asset for companies, and it should be protected as much as possible. The importance of information varies by the size of the company and the role that the information plays in the company's business model. Since information is so critical to companies, it is significant target for attacks. Shameli-Sendi et. al. (2016) argue that cyber threats are the leading business threat right after economic uncertainties. To protect the information within the company, managers aim to improve their security. Information security has been improved using security tools and training the staff to spread awareness of staff responsibility in protection of information (Baker et. al., 2007).

To identify security risks within organization, effective risk management process is required. Predefined process will make it easy to conduct risk management and make successful protection of information possible. Risk management process contains identification of risks, assessment of risks and taking steps to lower possibility of the risk to acceptable level (Stoneburner et. al., 2002). From these steps, assessment of risks is the most important part (Peltier, 2005). The goal of risk assessment is to link risks and assets affected by the risk together and prioritize them. Careful risk assessment protects the organization and enables organization to take actions against the threats. Risk assessment also helps organizations to implement preventive controls and safeguards against the risks.

Key components in information security risk assessment are assets to be protected, threats against the assets and vulnerabilities that expose assets. Assets are something of value for organization. Mostly these assets can be defined as information. Assets are identified within the scope of the assessment and their value and criticality are evaluated. Threat is something that might cause harm for the organization. Usually this threat is a person, but abstract concepts, such as nature, should be taken into consideration. Vulnerabilities are holes in the security system which allow unauthorized access to the assets (Wangen et. al., 2018).

Multiple different information security risk assessment processes are developed, but usually they contain three steps: context establishment, risk identification and risk analysis (Dhillon, 2007; Shedden et. al, 2006). The goals of these steps are to define the organizational context for the risks, identify the most important assets to be protected to allow prioritization of the risks, identify the threats and vulnerabilities affecting the assets and calculate the probability of occurrence and impact of the threat if it occurs (Whitman & Mattord, 2005). The information provided by these steps can be used to define risk management plans and management is able to justify the costs generated by risk management.

Whatever risk management approach is chosen by a company or organisation, it always contains the assessment of business-critical assets of possible threats, vulnerabilities, and measures that can reduce the risk to acceptable level (Baskerville, 1993). While deep understanding about the organisation in discussion and the information security field as a whole is important to most of the risk management methods, there has not been much research about formal knowledge representation of the areas that are relevant to information security risk management (Herzog et. al., 2007). Research has shown that in most of the cases where the selected risk management method has not worked well for the company was caused by management missing understanding of information security (Straub & Welke, 1998).

2.3 Challenges in information security risk management

Fenz et. al. (2014.) presented six challenges regarding information security risk management: (1) asset and countermeasure inventory, (2) assigning asset values, (3) failed predictions of risks, (4) the overconfidence effect, (5) knowledge sharing and (6) risk vs. cost trade-offs. Challenge 1 presents a concern that since individual fragments of information are connected to each other, the inventory of assets grows large. Hence, the environment gets complex when company or organization is growing. To enable sufficient risk identification, assets need to be categorized to inventory, so they can be analysed during risk assessment. Challenge 2 shows that it is hard to evaluate assets that are small, or which do not have straight monetary value. To tackle this issue the values should not be set to money, but to some other measure which indicates how much one asset is worth. This measurement should be defined by the company or organization based of the assets value in business process. Challenge 3 shows that prediction of attackers' interests might not be accurate, since interests tend to shift due time. In addition, definition of risks might be hard since the weight of assets change due time and the outcomes of risk realization might be unknown. Challenge 4 shows that managers tend to be overconfident about their assets, hence not all risks can be identified, or they do not get enough attention. To prevent this issue from realizing, risk management processes need to be improved to remove the overconfidence. Challenge 5 emphasizes the need of knowledge sharing among experts. Knowledge sharing reduces the cost of knowledge acquisition during risk management and improves the product quality. If knowledge is

not shared enough, the cost of risk assessment grows. Challenge 6 means that costs of countermeasures and mitigation activities should not exceed the loss of resources if a risk realizes. It is hard to estimate the costs if risk realizes but at the same time the cost of countermeasures should not be more than the estimated cost of risk realization.

2.4 DevOps and DevSecOps

In the research context I will be discussing about DevOps. It is a practice which enables flexibility and effectiveness for software teams. The core concept is about combining software development and operations. To achieve this, there are multiple instruction about how processes should be implemented, for example automation of building, testing and deployment of software, collaboration between development and operations teams and active knowledge sharing (Ebert et. al., 2016). Benefits of adopting DevOps practices into software teams are faster feature development and release time, more commits to codebase in daily basis, improved quality assurance and enhanced collaboration and communication. There are also drawbacks in adaption of DevOps. Since the practise requires active communication between teams, lack of communication blocks the whole adaption. To get the benefits of DevOps, a change in mindset is required from whole organization so the management can understand how the practise brings value for the organization. When talking about automation, there are multiple different tools that enable automated building, testing and deployment. Since there are multiple different tools available, the learning stack for the developers is very big (Riungu-Kalliosaari et. al., 2016).

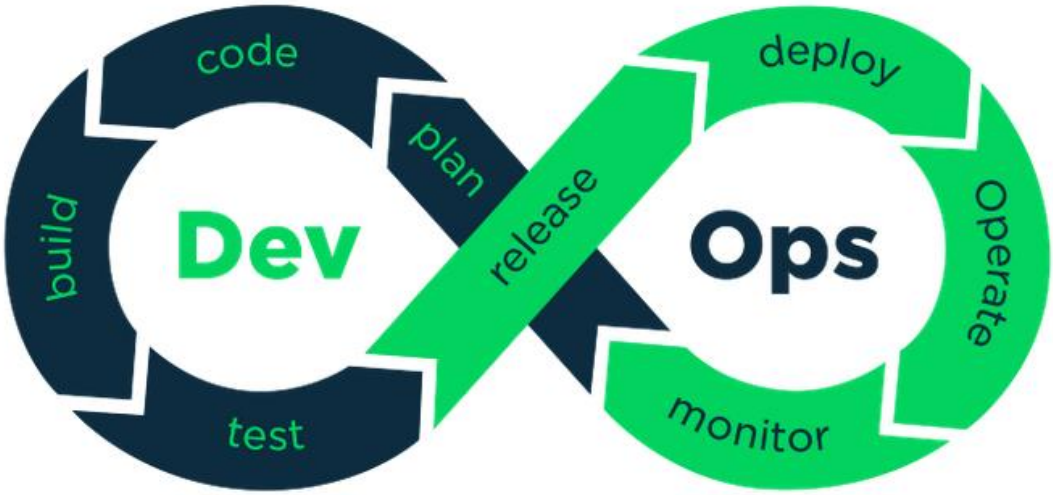

Figure 1. Illustration of DevOps cycle (Dutta, 2019)

When talking about information security, DevOps itself does not take information security into account. To integrate security aspects to DevOps practises, a new practise has been developed called DevSecOps. It is defined as expansion to DevOps, where security controls and processes are integrated into DevOps development cycle, and it can be achieved with collaboration between security teams, development teams and operation teams (Myrbakken & Colomo-Palacios, 2017). DevSecOps consists of 13 characteristics which will help companies with implementing information security while following DevOps practices. These characteristics are collaboration with team mentioned above (1), continuous knowledge sharing between the teams (2), security related feedback loop to enable quick security feedback to developers (3), continuous improvement of processes (4), active communication between security team and development team (5), setting clear responsibilities (6), establishment of trust between security team and other teams (7), experimenting with new ideas to improve security (8), leadership (9), ensuring commitment of staff (10), not to blame developers for security issues but help them fix them (11), hiring new personnel with security background (12) and full transparency inside the whole team (13) (Sánchez-Gordón & Colomo-Palacios, 2020). When these practices are integrated to DevOps, additional security assessments are not necessary since security is addressed in the DevOps practice itself.

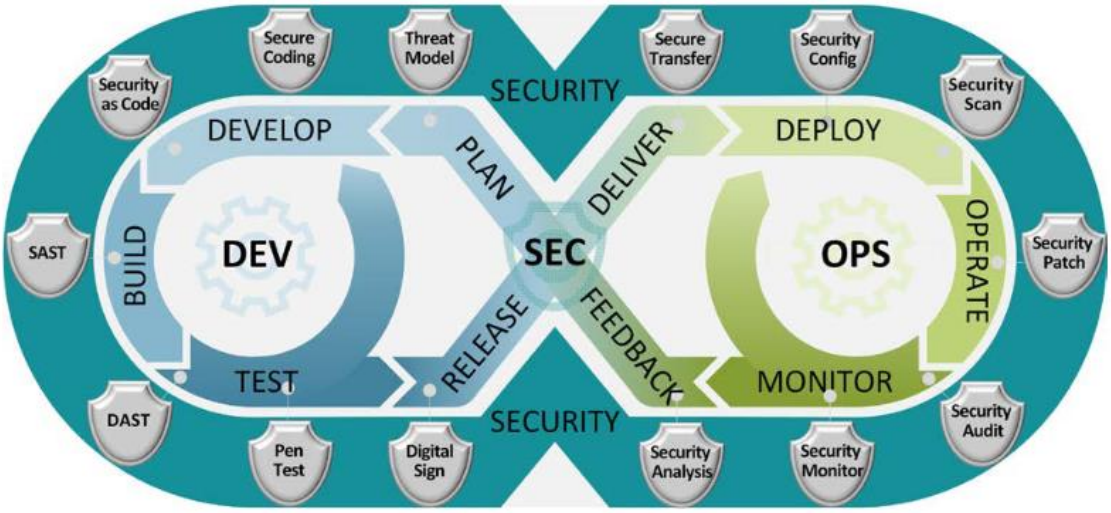

Figure 2. Illustration of DevSecOps cycle (Lam & Chaillan, 2019)

Mao et. al. (2020) present six significant factors which make it difficult to implement DevSecOps in practice. These factors can be separated into internal and external factors. Three internal factors which causes problems are (1) culture resistance, (2) high cost and (3) solidified organizational structure. External factors causing problems are (4) lack of DevSecOps experts, (5) lack of DevSecOps tools and (6) lack of mature DevSecOps solutions. They also argue that internal and external challenges influence each other. For example, culture of an organization is affected by employed experts and adopted solutions.

2.5 Overview of risk assessment frameworks

Information security risk assessment methods vary between industries, companies in the same industry and even inside an organization in different organization levels. Due to this variety, multiple different assessment frameworks have been developed (Aven, 2012). Even though there are multiple different assessment frameworks to use, it can be hard for an organization to find suitable framework to be used due to business requirements. A problem with many frameworks is that they follow general principles and guidelines and users do not get additional information regarding the implementation of preventing measures. The frameworks do not give enough information for managers to decide which implementations would be best suited for securing assets from defined risks (Sendi et. al., 2010).

2.5.1 CIRA

Conflicting incentives risk analysis (CIRA) is a method, which frames risks as conflicting incentives between stakeholders. The method was developed by Rajbhandari and Snekkenes to tackle the difficulty of getting reliable likelihood estimates for risks (2013). Incentives in CIRA means something that motivates someone to execute an action within the actor's capabilities and possibilities, which would give the actor advantage (Wangen, 2015). These incentives can be, for example asymmetry situations of information or moral hazard situations. The focus in CIRA is on the stakeholders. Method evaluates their actions and how the outcomes of these actions affect organisations' assets (Blakley et. al., 2001).

CIRA is developed based on game theory, decision, economics, and psychology. The strength of this method compared to other risk assessment methods lies in the threat actor and stakeholder assessment. Assets for the risk assessment are identified for each stakeholder according to utility and the method does not take business-related activities into account. On risk estimation, method avoids probability calculations and instead the risk is estimated by utility from executing potential strategies with accompanying outcomes. On risk evaluation, risk criteria are defined by the risk tolerance of the risk owner. This means how the risk owner can do counteractions against the risk if the risk occurs (Wangen et. al., 2018).

In a study conducted by Rajbhandari and Snekkenes (2013.), a practical example of CIRA is provided. The process consists of 13 steps. In step one, the risk owner(s) is defined. For the risk owner(s), the persona is also described. In step two, the key utility factors are defined. These factors are something that the risk owner(s) finds valuable. In step three, possible strategies that might affect the factors are defined. These are the actions that might cause harm for the risk owner(s). in step four, roles or functions that could have a possibility to execute these strategies are defined. These can be some roles inside the organization or outside. In step five, for each role or function, a strategy owner(s) is defined. This is some person(s) which could have the role or could have access to the function. In step six, for each strategy owner(s), utility factors of interest are defined. This means the definition of important factors for the strategy owner(s). In step seven, the measurement possibilities for the factors are defined.

After these seven steps, two stakeholder categories are defined: risk owner(s) and strategy owner(s). In step eight, each stakeholder will give a weight to their utility factor. The idea here is to prioritize the factors. In step nine, each operation is evaluated against the utility factors and the difference is calculated. In this example, additive utility function of MAUT was used to estimate the affects to utilities (Dyer, 2005). In steps 10 and 11, estimates and calculations for the utilities if the strategy is executed against them is done. From these calculations it is possible to see how much the strategies effect the utility factors for stakeholders. In step 12, using the calculations, actual risks are determined. In step 13, the risks are evaluated. Here we can see the level of acceptance for a risk to the risk owner(s).

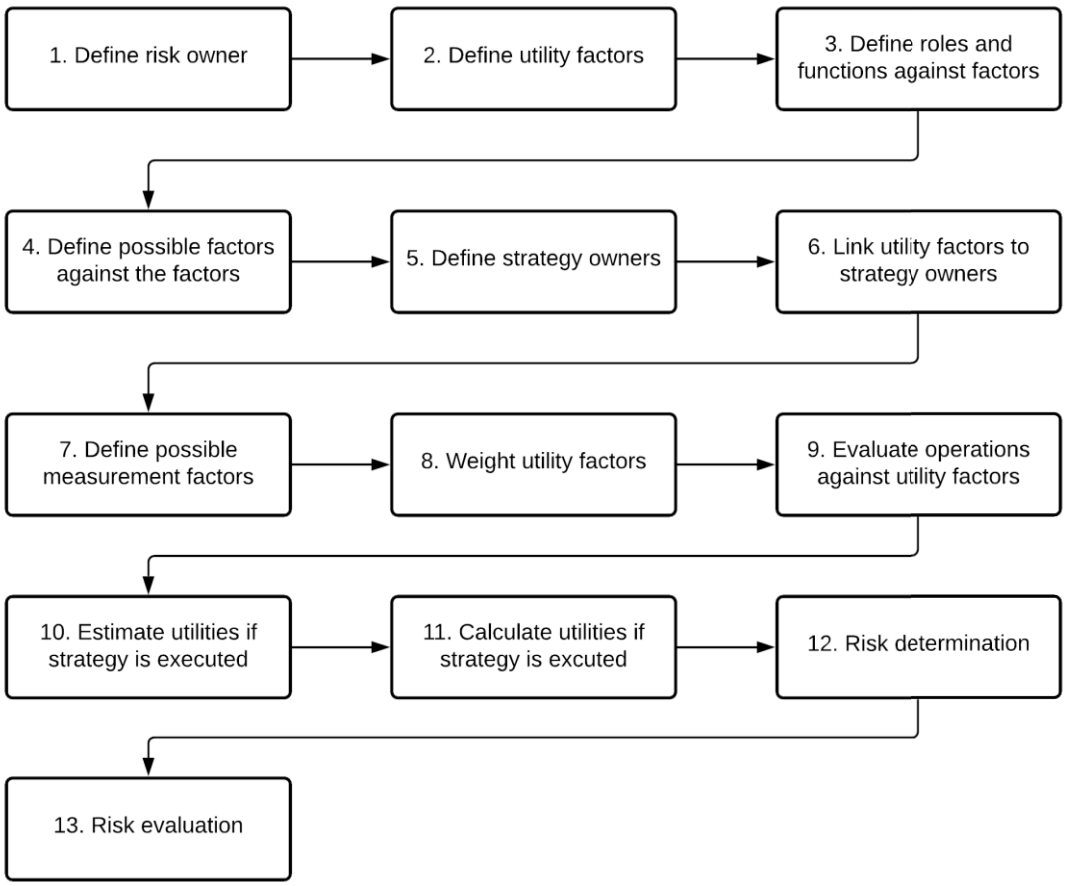

Figure 3. CIRA assessment process.

As seen above, the process focuses on the incentives of actors and utility factors of the stakeholders. The risks defined using CIRA are higher level risks and they do not give detailed descriptions of the risks in technical level. This makes the process time consuming for the organization, since all the risks need to be evaluated and no technical specification can be used. Also, CIRA requires an expert from the field to conduct the risk analysis, and this can be expensive if the organization does not have one inside it. Although, since the risk analysis does not contain technical specification, the risks can be reused in other departments inside the organization. A major disadvantage of CIRA is that the process does not follow any regulations or IT standards, which might be a deal breaker for organisations' for not choosing CIRA as risk assessment method (Agrawal, 2017). Another advantage of not using any technical specification is that the process can be used to define non-technical risks. For example, Agrawal and Szekeres (2017) used the process to define risks for community of practise organization.

2.5.2 CORAS

CORAS is a European project which is developing a framework for efficient risk assessment of business-critical systems. It focuses on integration of Unified Modelling Language (UML) in the risk management process. Unified Modelling Language is a modelling standard for object-oriented software design (Pooley & King, 1999). In this context, CORAS supports the practical use of UML in the context of security and risk assessment. The framework consists of four key points: A risk management process based on the AS/NZS 4360 standard, a risk documentation framework based on the ISO standard RM-ODP, an integrated risk management and development process based on UP and a platform for tool-inclusion based on XML (Jacobson et. al., 1999). CORAS covers business-critical systems in general, but places wight on information security. Information security includes for example achieving confidentiality and integrity of Business-critical systems (Stolen et. al., 2002).

Risk assessment process in CORAS framework consists of five steps: identify context, identify risks, analyse risks, evaluate risks, and treat risks. Aagedal et. al. (2002.) provide a practical example of the risk assessment process. The first step of the process is the identification of context. First part of this step is to identify the area of concern. Objective of this part is to think about possible scenarios which would affect important assets. Second part is the identification and evaluation of assets. Objective of this part is to identify what are the assets that are relevant to the scenarios defined in the first part. Third part is the identification of security requirements. The objective of this part is to identify the security requirements to protect the assets defined in the second part. In the end of the first step of the assessment process the scenarios, assets and requirements have been defined. The second step in the risk assessment process is the identification of risks. This step consists of identification of threats and vulnerabilities against the assets.

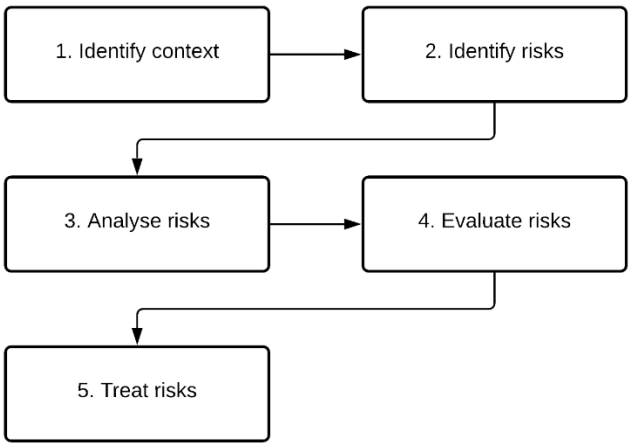

Figure 4. CORAS assessment process

Third step in the risk assessment process is the analysis of defined risks. First part of the step is evaluation of consequences and impacts. The objective of this part is to identify the level of importance for consequences and impacts of risks. Second part is the evaluation of possibility of occurrence. Objective is to determine how likely the risk will realize. Fourth step of the risk assessment process is risk evaluation. This step consists of five parts: determination of risk level, risk prioritization, categorization of risks, determination of interrelationships between category themes and prioritization of resulting themes and risks. Last step of the risk assessment process is risk treatment. This consists of identification of treatment options and assessment of alternative approaches.

Stamatiou et. al. (2003) conducted a study, where CORAS was used to conduct a risk assessment for telemedicine service. Their study shows that the framework improves risk analysis process since the understanding about the target of evaluation is improved by specifications of how it is structured and how it behaves. On the other hand, Fredriksen et. al. (2002) argue that the process depends heavily on experienced risk analysists. They also found out that sufficient input of documentation, including models, was critical to obtain valuable results.

2.5.3 ISRAM

Information Security Risk Analysis Method (ISRAM) is a risk assessment method developed by National Research Institute of Electronics and Cryptology and the Gebze Institute of Technology (Karabacak & Sogukpinar, 2005.). Since software has evolved from standalone applications to distributed solutions using multitasking and distributed processing, a risk assessment method was needed to evaluate risks in complex environments. The idea is to allow evaluation of complex systems by letting managers and staff participate together to the risk analysis. The method is a quantitative assessment method, which does not contain complex calculations to avoid need to use an expert to conduct the analysis and to save time.

The overall process in ISRAM is based on two phase surveys. These surveys are independent from each other and they address the probabilities and consequences of defined risks (Vorster & Labuschagne, 2005). The process in detail consist seven steps: Identification of information security problem, listing and weighing factors that affect the probability of occurrence and possible consequences of the problem, conversion of the factors to quantitative survey questions, preparation of risk table for probabilities and consequences, conduction of the prepared surveys, calculation of single risk value and assessment of the results (Karabacak & Sogukpinar, 2005).

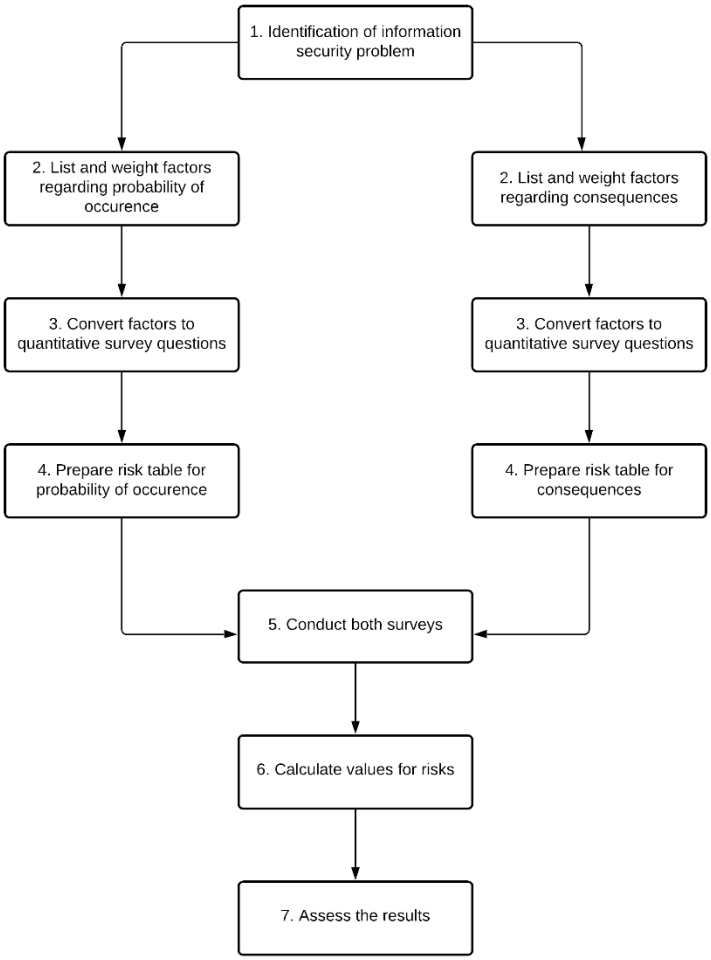

Figure 5. ISRAM assessment process

In a study conducted by Karabacak and Sogukpinar (2006), researchers used modified ISRAM approach to evaluate ISO 17799, provides guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization (Myler & Broadbent, 2006). The study indicates that the use of ISRAM is flexible since it can be easily modified to suit the situation and the modification does not take much time. In addition, use of software solution to conduct the surveys is optional, if the organization cannot use many resources for the analysis. Downside is that the process relies heavily to the participants. If the participants will not answer truthfully and accurately to the questions, the reliability of the analysis can be questioned. In addition, structure of the organization and the processes inside the organization can have on effect to the surveys, for example omitting some questions (Karabacak & Sogukpinar, 2006).

2.6 Overview of risk assessment frameworks for cloud environment

Even though the benefits of cloud computing are clear, so is the need to develop information security solutions for cloud computing. In addition to the challenges of developing secure information systems, cloud computing presents additional level of risk because services are usually outsourced to a third party. The externalized feature of outsourcing makes it hard to maintain for example data integrity and privacy, support data and service availability, and demonstrate compliance (Buecker et. al., 2009). Many of the risks associated with cloud computing are not new and can be found in organizations' today. Well planned risk management activities are important to ensure that the information assets are at the same time available and protected from threats and cleared of vulnerabilities (Mather et. al., 2009). In this chapter I will present few options for information security risk assessment frameworks associated with cloud environments.

2.6.1 ISGcloud

Information Security Governance framework for cloud environment (ISGcloud) is a framework developed to deal with specific features of cloud computing regarding information security (Rebollo et. al., 2015). The framework is process oriented and it is based on tasks which allow development of security governance structure supporting a cloud computing service. During the process, the framework maintains a continuous security governance approach, being aligned with existing proposals such as Control Objectives of Information and related Technology (COBIT) (Al-Sa'eed et. al., 2012).

The core idea behind ISGcloud is to define processes that systematize related security aspects, which provides organizations with an instrument for implementation, monitoring and management of information security (Rebollo et. al., 2015). The framework provides practical information to each stage of the life cycle of the cloud computing service easing its implementation and monitoring, allowing the integration and adaptation of standards (Silva et. al., 2016).

ISGcloud consists of six activities: planning, cloud security analysis, cloud security design, cloud implementation, secure cloud operations and cloud service termination. A research conducted by Rebollo et. al. (2015.) gives practical insight how the framework works in practise. In the first step, a new security governance structure is defined and planned to be built from scratch. In step two, security analysis for the example cloud environment is conducted. In step three, a new security design for the security governance is developed. In step four, the design will be implemented to cloud environment. In step five, the operation of the cloud is secured. The evaluation of the framework in the same study showed that the framework was useful and easy to learn to most of the participants.

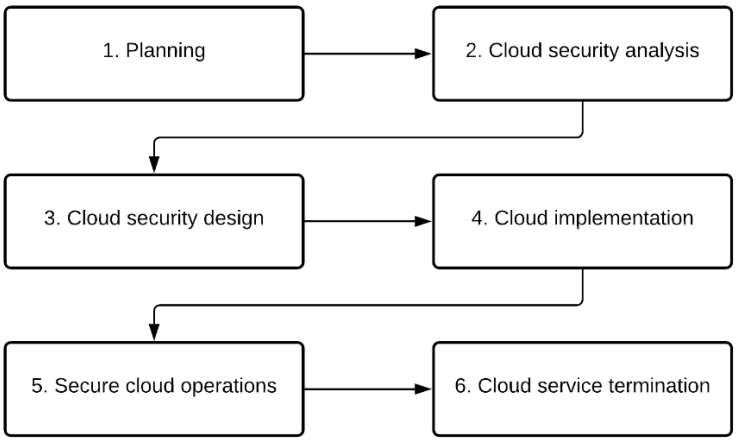

Figure 6. ISGcloud assessment process

2.6.2 QUIRC

Quantitative risk and impact assessment framework (QUIRC) is a risk assessment framework which defines risks as a combination of the probability of a threat affecting an asset and its severity measured as its impact. The method was introduced by Saripalli and Walters (2010). In their study they demonstrate how traditional security threat modelling can be related to the QUIRC calculations, via identification of security threat events. Also, Wide-band Delphi method is proposed as a suitable method for collecting data regarding risks affecting organizations' assets. The Delphi method is a forecasting technique developed by RAND Corporation (Stuter, 1996) to collect expert opinion in an objective way and arrive to conclusions based on that.

Security risks in QUIRC are linked with six key categories of security objectives (SO). These security objectives can be for example confidentiality, integrity, auditability, multi-party trust, mutual auditability, and usability in a Cloud platform (Saripalli & Walters, 2010). The framework defines an impact factor, which is the effect of a security threat event against organisation's assets, and the probability of occurrence for that event to derive a risk value. Impact factor is drawn from one of the six security objectives and it is combined using a weighted sum as function of its probability. Event probability is defined using known statistics, such as the amount of SQL injection attack reports. Using the Wide-band Delphi method, experts will rank the impact of risks and the probability of occurrence.

According to Djemame et. al. (2011), The advantage of QUIRC is that it enables comparison of information security between different cloud platform providers for vendors, customers, and regulation agencies, while they argue that the biggest challenge of this approach lies in its need for historical data for threat events probability calculation. A downside of QUIRC is also the fact that it does not consider specific security requirements as part of the factors in deriving the impact of different attacks. Security requirements are an important factor in security risk assessment, and hence the impact assessment of a threat must be based on the security requirements of the cloud tenants (Poolsappasit et. al., 2011). An important thing to consider in security assessment for cloud environment is to cover both the customization of the impact based on high-level business goals of a client and low-level functions of components in the network. This results in a specific, concrete, and accurate risk assessment. In cloud computing it has been known for some time that security risks differ depending on software architectural design patterns, thus requiring specific and clear security plans to mitigate the possibility of risk occurrence and the impact of the risk (Halkidis et. al., 2008).

2.6.3 Combining NVD and CVSS

National Vulnerability Database (NVD) is a popular and widely used database of vulnerabilities (Zhang et. al., 2011). In the database, the vulnerabilities are listed with a CVE-ID, which is a unique identifier for the vulnerability used to refer to it as a source. To this database, almost 20 new vulnerabilities are reported each day and by mid-2019, there were over 37000 entries of vulnerabilities (Frühwirth & Männistö, 2009). Each entry is public, and anyone can go look for them. Because the identifier is unique, it allows automation of vulnerability management and security measurement.

In entries listed in NVD, The Common Vulnerability Scoring System (CVSS) is used to help organizations' security managers in the prioritization of vulnerabilities by providing a metric for their relative severity. CVSS assigns each vulnerability a score on a scale of 0 to 10 where higher values indicate greater severity. CVSS was originally designed as a framework consisting of three different metrics: the base metric, which defines the general features of vulnerabilities, optional temporal metric, which represents changes in the severity over time, and the optional environmental metric, which defines context information that is unique to individual user, organization, or environment (Mell et. al., 2007).

Lenkala et. al. (2013) propose a framework for cloud environment, where NVD is used as a source of vulnerabilities and the risk assessment is conducted using formulas developed by Joh and Malaiya (2011.). The framework defines five states for risks: not discovered, discovered, disclosure with patch applied, exploitation, disclosure without patch and disclosure with patch not applied. Transitions for each state is defined in a matrix and initial probability for each vulnerability is defined. Using formulas developed by Joh and Malaiya, confidentiality risk, integrity risk and availability risk is calculated using data fetched from NVD. The study conducted by Lenkala et al. shows that security metrics defined in their framework can differ significantly, which shows that a comparison framework for comparing cloud providers is needed and important.

2.7 Experiences from risk assessment frameworks

Gaute Wangen (2017) conducted a study where different risk assessment frameworks were compared. It was found that the key criteria for selecting an assessment framework are content, context, experience and produced results. The study also showed that users of the framework prefer assessment frameworks which contain templates and examples. At the same time, templates produce extra paperwork, which was found a troublesome. Since frameworks require experience, if inexperienced risk analysist implements the framework, the produced outcomes may not be adequate for the context.

Taubenberger et. al. (2011) present their experiences from traditional risk assessment methods. They argue that quantitative assessment methods are based on data that is not reliable available in practise, standards do not have guidance on possibility of occurrence determination, frameworks do not take design of the system into account, assessment of the risks are not statistically accurate and they are conducted in reliable environments, low and medium risks defined during the assessment process are not mitigated due company constrains and the parameters for the risk environment are not accurately defined. They also argue that security requirement-based approach for risk assessment would be better solution than using traditional approaches.

2.8 OCTAVE Allegro

Operationally Critical Threat, Asset and Vulnerability Evaluation Allegro (OCTAVE Allegro) is a widely used risk assessment method developed by researchers at the Carnegie Mellon University in 2007. It was developed to identify, analyse, and prioritize information security risks (Liu et. al., 2009). Based on the results of OCTAVE Allegro risk assessment process, information security professionals can identify information security risks and create a prioritized list of mitigation strategies by developing security measures to reduce the effects of risk realization.

Alberts and Dorofee (2003) introduce how OCTAVE process works. The method consists of three phases: building of asset-based threat profiles, identification of infrastructure vulnerabilities and development of security strategy and plans. During first phase, the organizational view is created by focusing on people acting in the organization. During second phase, the technical view is created by focusing on the infrastructure used inside the organization. During third phase, organizational and technical view are gathered for evaluation. First the risks are defined from the views and then two workshops are held to propose protection strategy, risk mitigation plans and action list, and approve them.

Advantages of OCTAVE Allegro are easy to follow process with clear steps to follow during the risk assessment. The process insists experts to investigate areas that would have been otherwise not been checked, and templates and worksheets are useful tools to help with the assessment. Disadvantages include troubles with learning the process since it is found overwhelming for beginners, single phase consumes a lot of time and the results are not found satisfactory and it is easy to lose focus and prioritization during the process (Wangen, 2017). Muhammad Asif Khan (2017) also argues that OCTAVE Allegro is good and simple approach to risk assessment for small teams which have experienced employees working in them.

2.9 GBM-OA

Päivärinta et. al. (2014) introduce a risk assessment method based on genres combined with OCTAVE approach (GBM-OA). The process is iterative, and it consist of seven steps: Definition of stakeholders for security risk analysis, definition of risk measurement criteria, definition of producers and users of information, identification of genres of communication, development of information asset profile with genre properties, identification of containers and identification or risks and mitigation strategies. First, the participants for the assessment are picked by defined leader, preferably someone from management. Second, the risk evaluation scope and priorities are defined. Output of this step will help with the risk definition. Third, the genres are defined which represent for example people or units. These genres move information between each other using some method of communication and use the information for something. The definition of these communication methods is done in step four. Fifth, properties of all genres are defined. These properties can be used to find assets from the communication between genres. Sixth, containers for information assets are defined. The important thing in this step is to find out what assets lie inside the communication. Lastly, risks against the assets and mitigation strategies to prevent or mitigate the risks are defined.

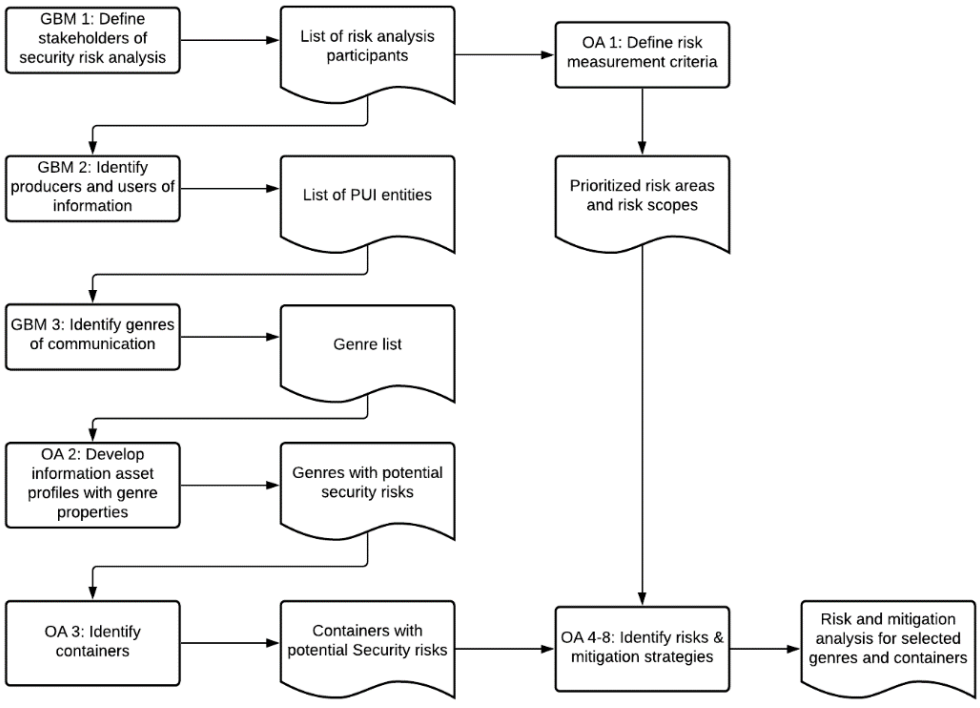

Figure 7. GBM-OA assessment process

Initial experiences of the framework were collected from three master's degree students who participated in a course in which the framework was introduced (Päivärinta et al., 2014). The students wrote learning journals, risk assessment document, reflective journals and conducted interviews to talk about their own experiences of using the framework. The evaluation pointed out three main topics: 1) It takes time to understand the terminology and risk assessment process, but after getting familiar with the framework it gives detailed organisation- and knowledge-oriented focus on risk assessment. 2) Focusing only to genres during the risk assessment ignores the security risks related to physical and electronic information assets and asset containers. 3) The framework was easy to use, structured and flexible. Even though the framework gives good insight on risks on organizational level, Päivärinta et al. (2014) want to point out that in big organizations prioritization of the genres may prove difficult. Organization might have thousands of genres that should be considered during the risk assessment, analysis, and documentation of all those genres would not be cost efficient and resources would be spent on definition of risks which would have minor or insignificant impact on the organization. Instead of trying to analyse all possible genres, organization should select which genres are business-critical and which genres might contain risks which would cause major losses for the organization.

2.10 Conclusion of the review

In this section I have discussed about information security risk management and frameworks developed to conduct risk assessment. Organizations rely on technological solutions to conduct their business efficiently. Due to this, lot of organizations' assets are vulnerable to attacks. Information security risk management is important working practice to secure companies' business assets and protect themselves against threats. Risk management consists of several components, and the one in focus in this thesis is risk assessment, which is the identification and evaluation of risks. There are several risk assessment frameworks available which can be used to conduct risk assessment in different contexts. These frameworks can be categorized as qualitative and quantitative frameworks. Qualitative frameworks focus on expertise of people working in the organization and the risks are identified by discussing about the environment and technological solutions used by the organization. Quantitative frameworks rely on statistical data about risks identified in the industry, evaluation of their cost impact and the probability of occurrence. With these variables it is possible to calculate the priority of risks. As in quantitative frameworks, also in qualitative frameworks it is important to prioritize risks, since in big organizations it is almost impossible to mitigate all identified risks, and some of them need to be accepted.

In the literature review I have introduced different frameworks which are suitable to basically any context, and I have also introduced frameworks specialized in cloud environment. Since organizations are starting to rely on cloud solutions to decrease infrastructural costs, there has been a need for risk assessment frameworks which take cloud environment characteristics into account. There is no strict rule which risk assessment framework should be used in given situation, but the selection depends heavily on the context of the case and the risk assessor needs to think about how different approaches would work in their case.

3. Methodology

In this section, I will introduce the study conducted in this thesis. The objective of this section is to discuss about how the study was conducted, what tools were used and describe how the research process was followed in the study.

3.1 Research questions

Research questions answered in this thesis are:

RQ 1.1: What kind of risk assessment frameworks are available?

RQ 1.2: What kind of risk assessment frameworks are suitable for cloud environment?

RQ 2: How to implement risk assessment framework GBM-OA in practice?

RQ 3: How well GBM-OA suits to case context?

Research question 1 was discussed in section 2. Question 1.1 is about what kind of risk assessment frameworks are available. The goal of the research question is to find some information about different frameworks and how they differ. The question is answered by looking into previous research conducted about risk assessment frameworks. Question 1.2 is similar to question 1.1, but the goal is to investigate frameworks which are tailored for cloud environment. Question is also answered by looking into previous research.

Research question 2 is about implementing GBM-OA into practise. The goal of the questions is to describe how to implement this framework to described context. The description of the context can be found from section 3.3. Answer to the question can be found from section 3.4.3.

Research question 3 is about experiences from the practical implementation. The goal of the question is to find out if GBM-OA is suitable risk assessment framework for the given context. Answer to this question can be found from section 3.4.4.

3.2 Research method

To find answer to the research questions, canonical action research (CAR) method was used. The method was first introduced by Susman and Evered (1978). The method is based on action research, which was developed in the aftermath of World War Two to take actions against social problems associated with battlefield experiences (Trist & Bamforth, 1951). After the issues were solved, action research has gone over major development and refinement. After 1990, action research was accepted as a legit research method in information systems domain. Several publications have been created to only address research conducted using action research method (Baskerville & Myers, 2004).

Canonical action research process is described in figure 8. It consists of five steps: diagnosis, action planning, intervention, evaluation, and reflection (Davidson et. al., 2012). Diagnosis is the entry point for the process. In this phase, justification for the research is defined. There must be a reason why this research should be conducted for this context. During second phase, the actions to implement change are planned. During third phase, the plan is executed, and the planned actions will be done. During fourth phase, the implementation process is evaluated. The objective is to identify how the change has affected the environment. During the last step, the researcher reflects the process and tries to identify the key learnings from the process to communicate to the scientific community to append general knowledge (Malaurent & Avison, 2016).

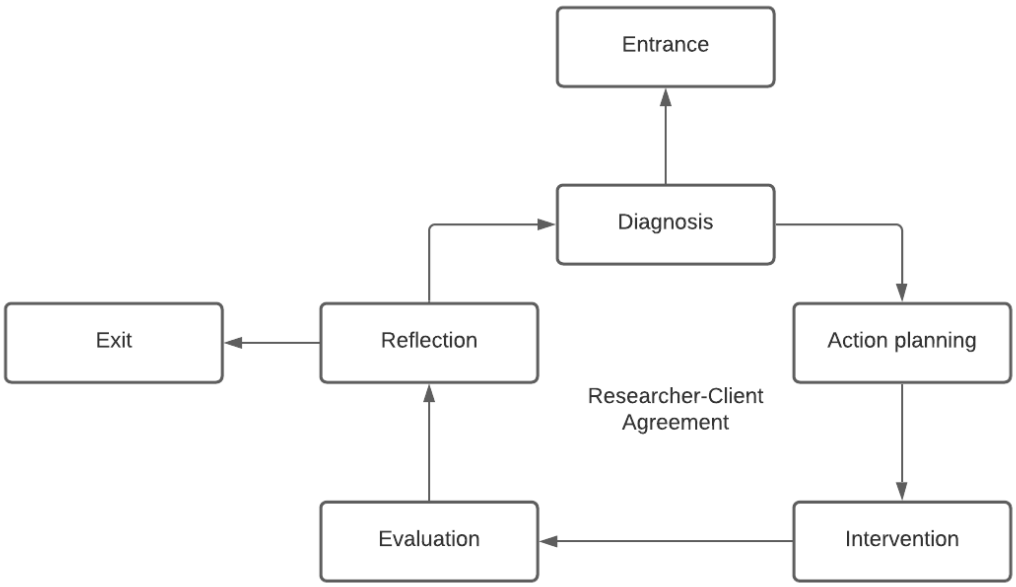

Figure 8. Canonical Action Research process

Olsson and Henfridsson (2005) provide a practical example of action research in development of context-aware application that transcend the mainstream design agenda in context-aware computing. During diagnosis phase, a collaborative workshop was held with researchers and practitioners and the key challenges in car infotainment systems. During action planning phase, actions to be done were defined to test how an interactional view of context would affect design adapted to their setting. During intervention phase, the prototype for the setting was developed. Evaluation phase took two months and during the phase semi-structured qualitative interviews were conducted to verify that the design principles were fulfilled. The key learnings from the process were discussed during the reflection phase.

To evaluate how well the selected risk assessment framework works in the given context, qualitative semi-structured interviews are used to collect data from research participants. Qualitative approach for the evaluation is selected because qualitative approaches contribute to understanding of the human behaviour in different contexts and in a particular situation (Bengtsson, 2016). Since this thesis is about empirical evaluation, to get data about experiences from the risk assessment framework from the assessment participants, semi-structured interviews are conducted. Using interviews, it is possible to get participants insights about the process and it is possible to reflect what were the good and the bad things (Horton et. al., 2004). Semi-structured interviews are the most common case of interviews, since it gives straight guideline to follow for the interviewer but also it gives flexibility to follow a lead which appears during the interview. In addition, semi-structured format allows free discussion between interviewer and interviewee which helps interviewee to give wider data to interviewer. It is also possible that a bond between interviewer and interviewee may be established which makes the interview situation feel lighter and the interviewee is able to answer truthfully and think the questions through (Kallio et. al., 2016).

3.3 Research context

Research in software industry is heavily depended on the context of the research. Results from one study may not be applicable to another since the context is different (Dybå et. al., 2012). According to Schatzki (2002), recognizing the influence of context is important, because it determines the phenomenon and shapes the practices within it. For this reason, I will introduce the context of this study. Target company of the study conducted in this thesis is referred as target company (TC) to prevent reveal of business sensitive information.

3.3.1 Continuous integration & continuous deployment

Continuous integration (CI) is a software practise where developers integrate code frequently, at least once in a day. It is popular practise in software development, since it allows merging small changes quickly and developers get fast feedback (Beck, 1999). Continuous deployment (CD) is a practise which aims to rapid delivery of software to customers using automated building, testing and deployment (Humble & Farley, 2010). Closely related to CI/CD is DevOps process. DevOps is a combination of development and operations and means culture shift towards collaboration between development, quality assurance and operations (Ebert et. al., 2016).

3.3.2 Case description

TC has established a service to centralize CI/CD solutions. The service is referred as target service (TS) to prevent reveal of business-critical information in this thesis. TS is an environment where projects are able to build, test and deploy software to their customers. Development, maintenance, and support for the service is handled by global team located on multiple time zones. Aim of the team is to support projects in CI/CD process and spread the DevOps working practices to developers.

TS environment consists of multiple different components, including version control, CI/CD tools and physical servers. Git is used as version control tool, Jenkins as CI/CD environment, Puppet for server management, Docker to provide container build resources for projects and Artifactory as artefact storage. These are just few examples of the components used in TS.

Cloud environment has been raising trend for few years and companies are starting to use or move to cloud solutions to outsource their infrastructure. Cloud allows independence of location and devices and it is highly available and scalable (Wyld, 2009). TS is currently using physical servers hosting a Docker swarm to provide resources for projects. In addition to TS provided swarm, projects are using their own physical servers as resources. TC has a department which is responsible for physical servers inside TC. Hence, TS is heavily dependent of that department. If problems occur in the servers, problems are reflected to projects through TS. To mitigate this risk, and due to the facts introduced above, TS team has planned to move from physical server environment to cloud. Using cloud solution, TS team has direct control of the environment and they are able to control it directly. Also, risks regarding maintenance of the servers and scalability can be moved from TS to third party.

3.4 Research design and findings

As described in section 3.2, canonical action research consists of five steps: diagnosis, action planning, intervention, evaluation, and reflection. In this section I will describe how this process is implemented in this thesis.

3.4.1 Diagnosis

First phase of the process is the diagnosis of the situation. As described in section 3.3.2, target service is planning to move from physical server environment to cloud. There are two cloud solution which are planned to be used in the future: in-house solution and Amazon Web Service (AWS). In-house solution would be customizable, and the control is completely inside TC. AWS is the leading cloud environment with flexible solution providing high availability, strong support for enterprises and scalable build, test, and deployment environment. AWS is accessible from both web browser and client console (Lee et al., 2010). In both of these solutions, security issues need to be addressed. Since TS provides a centralized CI/CD solution used by TC inner customers, project specific business sensitive information needs to be secured. Working in cloud environment is fairly new for TS team, need for risk assessment has been identified.

To identify what approach would be optimal for TS team, discussions with team manager and project manager were held. The objective of these discussions was to identify what framework could be used for the context of TS team. Since the team is small compared to other project teams in TC, it is important to find a lightweight solution which would not use many resources of the team. Also, the framework should be optimal for evaluation in this thesis. Conclusion of these discussions were to use GBM-OA approach described in section 2.9. Reasoning for this selection was that the workflow of the framework is clear, templates for the steps in the framework are developed and provided by the developers of the framework and the process is easily repeatable, which would allow usage of the framework in the future.

3.4.2 Action planning

The risk assessment process was split into three workshops. These workshops took one hour each. First workshop consisted of steps from GBM 1 to OA 2. Second workshop focused on OA 3 and the last workshop focused on OA 4-8. The reason for splitting the process into three parts was, that to run through the process successfully it is important that participants are active during the workshops. To ensure that participants will not be too tired to give their opinions about the subject at hand it was necessary to keep the workshops short, especially when the risks were identified.

The first step of the risk assessment process was about selecting who will be participating in the risk assessment. According to instructions of GBM-OA, one person is selected to be the leader of the process. This person should be someone from the management. Rest of the participants should have proper expertise to participate because the process relies heavily on the knowledge of the participants. To ensure successful completion of the process, discussions with the process leader were held to select suitable personnel.

The second step is to define scopes for the risk that will be identified during final steps. The goal is to focus only on strategically important areas. To get most out of the process, it is important to focus on the most important areas and not take all possible situations into consideration. The focus areas of the assessment were discussed with the participants during the first workshop session. The defined scope was reflected during later steps.

Third step begins the actual assessment actions. During this step, the producers and users of information will be defined. Definition of producers and users will give an overview of the environment and how information is moved inside the environment. Producers of information are players in the environment which produce some valuable information to some other player and the users depend on that information. This flow of information connects the players together and this connection helps the environment produce value. Hence, it is important to secure flow of information and make sure that no actor outside the environment can access the information moving inside the environment. On the other hand, to prevent misuse of information or unauthorized access it is also important to make sure that only the user(s) which are dependent on the information will get it and no other player inside the environment is able to access the information.

The fourth step consists of identification of genres of communication. The genres represent the flow of information inside the environment. The information is produced by producers of information and used by users of information. Together, producers and users of information form the chain in which the information goes through. The vectors which are used to transfer information between producers and users varies from physical copies to spoken exchange of information. To enable identification of informational assets it is important to identify what is the actual information moving inside the environment, how the information is exchanged between producers and users and what could possibly disturb or alter the flow of information. To successfully identify the genres, active participation is required since there might be hidden information moving inside the environment which is only known by one of the participants.

The last part of the first session was about defining detailed description of the genres and try to find out which of the genres have potential security threats. This step is important since it is hard to define all possible risks for all identified genres, so the genres need to be prioritized according to the threat probability and the scope of the assessment. The management representative plays important role in this step, since he/she can give information about how much resources there is available for mitigation activities, which can be reflected during the prioritization. If there are not many resources available, then genres possibly containing easy and quick mitigation activities should be prioritized and vice versa.

The second session was about focusing on identification of containers. As described in section 2.9, containers are detailed descriptions about how the genres move between producer and user of information. Using the containers, it is possible to see what risks could affect the movement of the information from producer to user. Inside the container description the movement of information is considered from both producer and user point of view. Also, the people or roles involved in the movement of information are defined. Diagonal matrix and Genre list defined during the first session will be used during the identification of containers to keep in mind the whole picture of the environment. Same roles will be participating in the second session as in the first session and one hour will be reserved for the session. Before the session, researcher prepared the container templates for all genres defined in the genre list to reduce the amount of time used for copying templates multiple times during the session.

The third session was about actual risks connected to the information that is moving inside the environment. During the third session, participants were discussing about the actual risks inside the containers and try to find possible follow-up actions on the risks. In the risk assessment, quality is more important that quantity. This means that we tried to identify few risks as detailed as possible rather than trying to identify large quantity of risks with few details. Also, to get as much value from the session as possible, participants were focusing on risks that could be mitigated. In practice, participants selected one or two containers defined during the second session and tried to identify risks that could be mitigated. At the end of the session participants needed to decide if they wanted to have another session for identification of risks or if they want to stop. It is not necessary to identify every single risk in the environment since we wanted to find out the most critical ones that need to be fixed or mitigated first. Because of this, participants needed to decide if the defined risks were enough for now or if there might be something critical still hiding inside the containers.

3.4.3 Intervention

In this section I will describe how the planned actions were executed. Notes taken from the assessment sessions can be found from appendix A. Examples of outputs from each session are also provided. The outputs are described in abstract level due to confidential information contained in the outputs.

During the first assessment session the process was executed from GBM 1 – OA 2. At the beginning of the session, a quick recap about the process steps was done to motivate and inform the participants about what we are doing during the process. Document was prepared and pre-filled by the researcher to save time. Risk areas and scopes was predefined by the researcher and accepted by the participants. Most important parts of the session were the identification of producers and users of information and identification of genres of communication. Diagonal matrix and detailed genre list created during the session. The participants were not very active at the beginning of the session because the session was scheduled after a long meeting and there was not enough time given for the participants to recover from the meeting. Participants did active after a while and discussions started to flow. The biggest challenge during the session was to stay inside the scope accepted at the beginning of the session. It is easy to start defining producers and users of information and genres about the whole environment, but to focus on singular area takes away most of the parts from the whole picture. But even with this challenge the participants were able to define diagonal matrix of the producers and users of information and the genre list within the scope and they can be used during following steps.

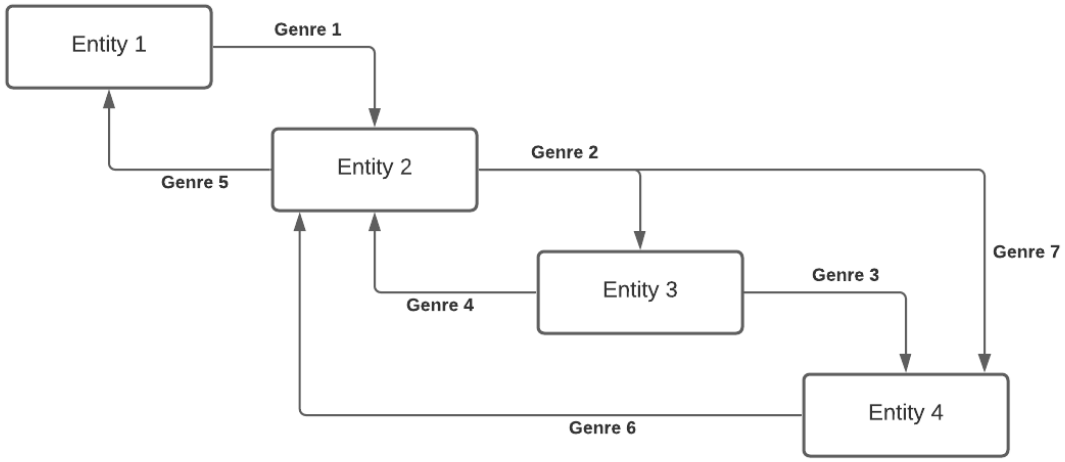

Figure 9. PUI matrix from session 1. Details have been changed due confidentiality.

Source/Producer	Content & communication genres	Audience / User(s)	Owner(s)/Responsible(s)	When is communication done?	Where does communication take place?	How do people communicate / share knowledge?
Entity 1	Genre 1	Entity 2	Entity 1	daily	Version control	Source code
Entity 2	Genre 2	Entity 3	Entity 2	Weekly	Email	Email
Entity 3	Genre 3	Entity 4	Entity 3	Monthly	Cloud	Documents

Table 1. Genre list from session 1. Details have been changed due confidentiality.

The second session started faster than the first session, since the participants were already aware where we left off last time and what we will go through during this session. A quick recap of the outcome of the first session was done at the beginning to get everyone on the same page if someone would have forgotten where we left off. The researched had done manual copy work for the container template to save time. Each genre from the genre list was gone through and the container was filled for each genre. The participants were able to define a container for each genre in the list and they can be used in the following third and last session. At the end of the session a quick peek on the following session was done to give participant heads up about what we will be doing in the third session.

Third session started late due to extension of meeting before the session, but the start was quick since the introduction of the session was done at the end of the second session. Risk identification was done by participants selecting few containers and discussing what risks could be found inside the containers. After risks were found, risk worksheets were filled for each risk. While filling the template, participants had hard time understanding what each part of the template was meaning. After some discussion, participants found consensus about the meanings and they managed to fill the worksheet for all risks except the last one, because there was not enough time. The last worksheet was filled by participants giving their own input by email and researcher filled the missing parts using the answers given by the participants through email. This session concluded the risk assessment process.

Genre 1	**Information Asset Risk Environment Map (Technical)**	**Genre 1**	**Information Asset Risk Environment Map (People)**
Internal		**Internal personnel**	
Container Description	**Owner(s)**	**Name of role / responsibility**	**Department or unit**
Container description from internal perspective	Entity 1	Relevant roles from entity 1	Entity 1
External		**External personnel**	
Container Description	**Owner(s)**	**Contractor / vendor, etc.**	**Organization**
Container description from external perspective	Entity 2	Relevant personnel from entity 2	Entity 2

Table 2. One example of containers defined in session 2. Details have been changed due confidentiality.

To answer the research question 2, this framework provided one possible implementation of risk assessment in practice. To summarize the assessment process, first the participants defined the environment and how the different players in the environment are connected to each other. This gave an overview of the whole environment to the participants which was reviewed when the assets were identified. Second step is to identify what are the assets that need to be protected. Third step is to identify what threats would cause harm to those assets and how can we protect them against those threats. As said, this process is just one possibility and it might not suite for all environments.

Genre 1	INFORMATION ASSET RISK WORKSHEET		
Area of concern	Concern (original replaced due confidentiality)		
(1) Actor	Actor against the genre. (original replaced due confidentiality)		
(2) Means	Means how to act against the asset. (original replaced due confidentiality)		
(3) Motive	Financial gain / Cause harm to project / Waste resources for personal use		
(4) Outcome	☑ Disclosure ☐ Destruction ☐ Modification ☐ Interruption		
(5) Security Requirement	Confidentiality / Integrity		
(6) Probability	☐ High ☐ Medium ☑ Low		
(7) Consequence	Possible consequences if the risk realizes. (original replaced due confidentiality)		
(8) Severity	**Impact Area**	**Value**	**Score**
	Reputation & Customer Confidence	High	5
	Financial	High	4
	Productivity	Medium	3
	Safety & Health	Low	1
	Fines & Legal Penalties	High	4
	Accreditation	High	4
		Relative Risk Score	21
(9) Risk Mitigation			
☐ Accept	☐ Defer	☑ Mitigate	☐ Transfer
Actions	Decided mitigation actions. (original replaced due confidentiality)		

Table 3. One risk defined in session 3. Some of the details are changed due confidentiality.

3.4.4 Evaluation

As described in section 3.2, to evaluate the risk assessment framework in context of centralized CI/CD environment, semi-structured interviews were held with the participants. Questions presented in the interview are listed in appendix 5.2. During the interviews, the interviewer was taking notes about the answers and after the interview was done, the notes were sent to interviewee to check that the notes are correct. The interviewees could also modify them if found necessary. This was found necessary, since interviewer was not able to record the interviews according to guidelines of the TC, and to verify that the participants can confirm that they have answered as pointed in the notes. References to the answers provided in this section are not pointed to any specific role to protect anonymity of the participants.

Before the actual risk assessment work was started, an introductory session was held for the participants to familiarize them with the framework. Initially the participants felt that the framework is heavy. There are multiple steps that need to be taken before the actual risk definition can begin. Participants were concerned that we would be spending too much time on filling pre-defined templates which would not give any new value for the team.

"*I felt that it required us to fill lots of stuff to pre-defined templates.*"

"*There was lot of new stuff, so it was hard to understand the overall picture in the beginning, but I understood that all these steps are necessary to get to good results.*"

Since the framework is defined with detailed steps from beginning to actual risk definition, participants felt that this assessment process is strict, and it does not have room for flexibility. Terminology used in the framework was confusing, especially the term "genre" caused confusing in participants. The framework contained lot of new things for the participants, hence it was hard to understand after the introduction. To counter this concern, participants hoped that they could have had an example from previous risk assessment with this framework to give practical example how the steps of the framework should be executed.

"*Initially it was hard to familiarize with the framework, especially with the terminology used in it."*

"*Example from previous risk assessment using this framework would had maybe help participants to understand the process better."*

On the other hand, some participants thought this as a good thing, since we do not have to spend time on defining how we want to conduct risk assessment, since the steps are already defined. Also, since the steps were defined in detail, income and outcome of each step was clear. Because we do not have to spend time on defining how the steps should be executed, we can focus on the actual assessment without spending time on things that do not give any value to the assessment. All the participants agreed that the framework is a good thing to try out in this context and it is needed for the environment, but they were not sure if it is suitable.

"*Framework will provide valuable information without spending too much time.*"

"*I felt that this is a good thing that should be conducted to our environment.*"

"*All in all, I felt that this is a good framework to try out in our environment.*"

Since the answers presented above are based on the knowledge from introductory session, the participants were asked about their feelings when the assessment started to see if their feelings had changes when the actual work started. First steps of the actual work in the framework (PUI matrix, genre list) were found important since they give an overview of the environment and they help when thinking about where the risks would be coming and how they would affect the whole environment if risks realize. It was found that it is especially important to understand how the different entities in the environment are linked to each other. Risk of losing focus and getting sidetracked during the assessment was presented as the main risk that could cause failure of assessment.

"*I feel that it is important to understand who is interested about who and how different players are linked to each other.*"

"*There is always a risk when conducting risk assessment that we get sidetracked and lose focus, so I feel that this risk was also present at the beginning of the assessment.*"

One interesting concern was that since the team is making big changes and moving to new infrastructure, the team does not know what the impacts of risks are if they realize. This shows the importance of people involved in risk assessment, since it is possible that the assessment fails because the participants do not have necessary understanding of the environment in security point of view. The concern was also verified by the participants since they were worried about how they can bring value to the assessment, since they are not confident in their own expertise in the field.

"*We are moving towards big changes which we are not familiar with, so we are not sure what are the impacts if the assumptions realize.*"

"*We know basic things, like what would happen if cloud VMs would crash of networks would go down. We are able to contribute only in that level, but we don't know what actual problems would arise in cloud environment.*"

After the initial feelings about the framework were collected, participants were asked to describe their feelings the after the assessment when the results are not taken into consideration. Participants were worried that this assessment was one more process which showed that these are the problems which we have, and the team is not going to do anything about them. The team already has a lot of documentation and the outcomes of the framework can get lost with the other documents. During the assessment sessions we had to stop the work to find out what some parts mean, for example the impact definitions in asset worksheet. These interruptions caused loss of time in the sessions and the flow of discussion was lost. The concern about lack of expertise was also raised after the assessment, since participants were not sure if we were able to define correct measurement metrics for the risks, since participants did not have detailed technical understanding of the new environment.

"*I felt concerned that this process is just another discussion where we find problems, but we won't be doing anything to fix those problems.*"

"*We found several unclarities like how to write things down, but we were able to complete the assessment.*"

"*I was concerned about if we were able to define metrics for the risks correctly, since we are lacking expertise in cloud platform.*"

The participants were surprised how little time the assessment took. We were able to find relevant risks without spending much time. This was a surprise to the participants since initially the framework seemed heavy, but at the end it was lighter than it seemed. In addition to the risks found in the assessment, participants also got a good understanding about the environment, since we had to think about how different producers and users of information work together. People involved in the assessment had experience from other risk assessment frameworks and they felt that GBM-OA is the least heavy and time consuming when compared to other risk assessment framework they had used.

"*All in all, I felt that the process went well, and I was surprised how little time it took to get to these results.*"

"*After the assessment we got a good picture of what the future infrastructure will be, and the framework was helpful in achieving that.*"

"*I feel that it is important to understand who is interested about who and how different players are linked to each other.*"

Results of the assessment were not surprising for the participants. They already had some ideas about what kind of risks are present, so it was expected that the results were not surprising. Value provided by the framework was the prioritization since the risks were not prioritized before. One participant compared the results to previous experiences with other frameworks and he/she thought that the other frameworks would have produced similar results. Since the framework gives weight to participants expertise and understanding of the environment, participants thought that we are not able to verify accurately if the results are correct, since they are mostly assumptions. Team can verify them only if they realize. In addition to risks themselves, participants were able to get new insight about the environment, which was additional value created by the framework.

"*The results were not surprising.*"

"*We were able to get a good overall picture of the environment and map the risks to responsible people with proper mitigation plans.*"

"*We can't really say if the results were right or wrong, since they can be verified only if they realize, since they are mostly assumptions.*"

When participants were asked about their opinion about the most valuable and invaluable steps, the opinions were very divided between participants. PUI matrix was seen valuable since gave good overview about the environment and how the team communicates with the stakeholders. Information containers gave insight about how the information is moved from producer to user and which people are involved in the process. Information asset worksheets were found valuable since they gave wide description of the risk, it helped with risk prioritization and mitigation activities were defined. At the same time, each of these steps were criticized. Templates were found to be compelling to fill due to repetition, information containers were found to be unnecessary work, impact areas in information asset worksheet were too abstract and participants had hard time to stay focused on the subject. At the end it was found that each of these steps are necessary to successfully complete the assessment and none of them can be left out. With these statements it is hard to say if any of the steps in the framework would be useless or invaluable.

"*The most valuable part was the definition of PUI matrix, where we discussed about our environment. It's good to think about how we collaborate with our stakeholders.*"

"*The information containers gave us good understanding about all pieces of our environment, which helped us to get common understanding of our environment.*"

"*Information asset worksheet was the most valuable part of the framework, but I don't find the other parts unnecessary, since they helped us in risk definition.*"

"*Describing information assets is not fun work and we had hard time to find suitable words to describe the assets, so I found it to be hard to stay focused on the subject.*"

"*Impact areas in the worksheet were too abstract and I don't think they are suitable for every scenario. They should be modified regarding the context.*"

"*The templates were very heavy, and we had problems with understanding what different parts mean.*"

When talking about which roles should be present in the assessment, participants found it critical that one participant from each producer and user of information should be present. They could give their own insight about how information is used and how they are responsible of genres in their opinion. Product Owner was found to be very important role to be present since he/she is doing the high-level prioritization and is actively communicating with the stakeholders. Number of engineers working on actual implementations was also found important, since technical insight and understanding was found to be key success factor in definition of security risks. At the same time, it is important that there are not too many participants involved in the assessment since that would slow the assessment process down and delay other daily tasks. Scrum Master was found unnecessary since technical details are not his/her area of responsibility. Participants also suggested that the number of participants should be adjusted in each step of the framework.

"*It is really important that Product Owner is present in these discussions, since he's the one who does the high-level prioritization about what we will be doing.*"

"*Scrum master is not necessary role in this process, since technical details are not his responsibility.*"

About how well the framework suits in context of centralized CI/CD environment (RQ 3), participants felt that it does not suit well as it is. Even though it brings value with definition of environment and risks, it is too strict and has too many steps to be executed every now and then. It should be modified so that it would be more lightweight with fever steps and it should be integrated into the development process instead of being individual process. Participants felt that the framework does not give enough value as separate process but if integrated to the development process it would give the team more value. In addition to value creation, participants felt that they do not want any more additional documentation and filling of all the templates is compelling. Team already has much documentation, so saving results as additional documentation is not recommended. Participants liked the fact that they did not have to spend much time for the assessment, but modification to continuous process was found to be hard.

"*The framework was not suitable in our context as it is, but it should be integrated into our development process. I feel that the assessment doesn't give value to us if it is separate discussion outside development work.*"

"*Changing this framework to continuous process needs to be discussed, since I don't find it easy to modify this process to continuous process.*"

"*I don't need any more documentation where we just write down issues and leave them there.*"

Improvement suggestions were collected from the participants and the biggest improvement areas were the structure of information asset worksheet and the iteration of the framework. One of the concerns regarding information asset worksheet template was the impact areas. The areas differ depending on the context of the assessment and the framework does not take this into account. It was suggested that there would be a step in the framework where the participants are requested to discuss what are the most important impact areas which should be used when the risk impacts are being evaluated. This could be additional step in the framework, or it should be integrated into one of the steps. Suggested change is presented in figure 10 below. The framework also indicates that the process can be done iteratively, but there are not any instructions about how often the process should be iterated and how it should be iterated. Hence the users of the framework must take time to figure it out themselves, which does not give much credit to the framework. Some instructions or examples should be provided in the framework description.

"*It would be useful to have a step in the process where participants define most important impact areas which would be used when risk impacts are defined.*"

"*There could be instructions about how to make the process continuous. Also, it should be defined how often the process should be iterated.*"

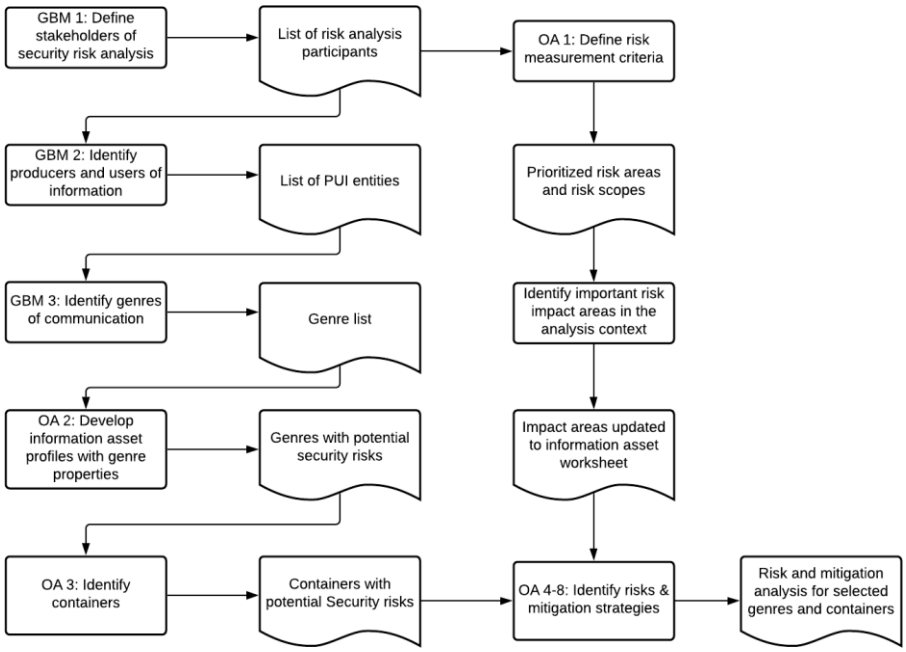

Figure 10. Suggested GBM-OA assessment process.

In conclusion, based on the discussions had with the participants it can be stated that the framework provides additional value with the risks and mitigation actions, but it is not suitable to centralized CI/CD environment without slight modifications. The main concern is that the assessment process should be integrated to development process, so it would be part of daily work. Iterating the framework as separate process will consume time from other activities, and the team does not want that the results of the process would be documented as a separate document since it would drown in the stack of other documentation.

4. Discussion

Since successful DevOps practices already require knowledge about multiple different tools, information security should not be added as additional practice to DevOps practices. It should be integrated into existing solutions or integrated into DevOps practices. In section 2.4 I have discussed about DevSecOps and how it can be used to integrate security aspects to DevOps practices. One of the problems in information security risk assessment found in this study was that the assessment process was found as an additional process outside development and operations. Adaption of DevSecOps practices could solve this problem in the TS on the other hand, adaption of DevSecOps in an organization requires implementation of DevOps and the practices described above. This is lot to take in and it requires resources. This may be a reason why organization would not want to use DevSecOps, but instead use just DevOps and conduct security related assessment and audits now and then. As noticed in this study, this additional security risk assessment felt compelling for the people participating in the assessment and they needed to stop their daily work to participate. This is a tradeoff that needs to be discussed inside organization.

When talking about DevSecOps, it is important to make sure that the security related activities do not disturb development and operations work. Since GBM-OA is individual process now, it should be integrated into development. To enable this, the framework should be split into individual steps, which would be executed at some points of development. For example, when a new feature is planned, it should be evaluated against different genres. Deployment of features can be evaluated against different containers. These possible integrations would make the framework as a natural part of daily work.

At the end, it is management decision how information security will be handled in a company or organization. If management does not care about information security, consequences may be severe. This can be seen from latest news about security breach in psychotherapy center Vastaamo, which turned public in September 2020. The first breach happened in 2018, but management decided to hide the event from public. When the attackers noticed that they have managed to steal confidential patient records, they started to blackmail the company for ransom. This could have been avoided if management decided to be transparent about the first breach and improve their security measures. This is a warning example that information security should be taken seriously, and resources should be allocated to ensure confidential information is secured.

4.1 Reflection

GBM-OA is based on how the information moves inside the environment from producers to users, and how that flow of information can be compromised. Without wide understanding of the environment, the framework does not give much value to the users. Hence the participants had to really think about what information the team provides and who are the actual users of that information. This raised interesting discussions between the participants, and it was clear that the participants were not completely aware who are responsible of different genres. This outcome raises a concern that if the results of the assessment are valid since the foundation of the assessment was fragile from the beginning.

DevOps is swiftly developing culture nowadays since companies are continuously trying to develop faster and more automated way to integrate development and operations together. To do this efficiently, teams are required to integrate multiple different solutions and tools together to achieve this goal, for example build and testing tools. Ebert et al. (2016) present a list of different automation tools available to create efficient CI/CD pipeline. Even though it is a good thing that there are multiple solutions available to build CI/CD pipeline, the amount of expertise required from DevOps engineers is growing. It is not enough anymore that engineers are experts of one or few tools, but engineers need to know how to use multiple tools. A study conducted by Lwakatare et. al. (2019) shows that even though the team would consist of experienced engineers, adaption of DevOps principles in practice was found compelling and they struggled with the learning curve. They also state that if the team is not professional enough in different DevOps tools, information security of the environment will get compromised.

The results from this study show how the DevOps mindset reflects to information security risk assessment. Jaabari et. al. (2016) presents a list of DevOps practices that should be implemented when adopting DevOps into company or organization. These practices show how important it is to automate everything from software development to deployment. Hence, developers aim towards automation and processes affecting software development should be integrated into either software development cycle or automation. Because of this way of thinking, participants felt compelled about separation of security risk assessment from development.

In section 2.3, I have presented different challenges regarding information security risk management. In this study, GBM-OA provided some solutions to these problems. On the other hand, some problems were clearly visible in the framework. Challenges 1 and 5 are taken into consideration in the framework. Challenge 1 was about inventory of assets growing larger and larger if the assessor tries to identify everything that might be an asset to the organization. GBM-OA tries to stick in the high-level flow of information, and details are only talked about during last steps of the framework. In addition, framework emphasizes the focus of the assessment, and it is important to keep the focus during the assessment, so there would not be too big inventory of assets after one run. Challenge 5 was about knowledge sharing between experts. It is necessary to share knowledge between experts to reduce cost of knowledge acquisition during risk management. At the beginning of GBM-OA the leader of the assessment selects which personnel will participate in the risk assessment. Idea here is to select people with different areas of expertise to make the pool of knowledge in the assessment wide. This is very important, since the framework relies on expertise of the participants.

Challenges 2, 3, 4 and 6 were visible also during this study. Challenge 2 showed concern that it is difficult to set meaningful values for the risks. As seen in the evaluation of the framework, there should be a step in the framework which would help the participants in definition of key impact areas and definition of risk values. Challenge 3 Showed that it is difficult the predict how the threats would attack against the assets, since the focus of interest changes due time. This challenge is not considered in the framework. Challenge 4 showed that management tends to be overconfident about their assets, and every critical risk is not taken into consideration. Since representative of management is the one leading the assessment, this challenge is clearly visible. Challenge 6 showed that the costs of countermeasures should not exceed the possible losses if a risk realizes. Framework does not take this into account, since only thing that is considered is that how the participants would like to handle the risk. They could accidentally or on purpose define too radical countermeasures.

At section 2.4, six challenges regarding practical implementation of DevSecOps culture were introduced. These challenges are similar to challenges presented for GBM-OA framework. For example, successful information security risk assessment with GBM-OA requires participation of security experts, since the framework relies on experience of the participants. In addition, framework requires that the participants need to think about security as part of their development work. If organization has successfully implemented DevSecOps practicalities in their development work, it is easier to conduct successful risk assessment, since the organization already has experienced employees and required security mindset. Since security is a natural part of software development in DevSecOps practise, GBM-OA should be easy to integrate into security related work.

4.2 Answers to research questions

First research question was about **what kind of risk assessment frameworks are available** and **what kind of risk assessment frameworks are suitable for cloud environment?** Risk assessment frameworks can be divided into two categories: qualitative and quantitative methods. Qualitative methods focus on expertise of people and the risks are identified through discussions. Quantitative methods focus on possibility of occurrence and losses if risk realizes. Risks are calculated according to estimates. Risk assessment framework used in this study, GBM-OA, is an example of qualitative method. One quantitative framework introduced in this paper is ISRAM. For cloud environment, additional layer of security needs to be taken into consideration, since cloud services are in many cases provided by a third party. Hence, it is important to make sure that the selected provider is taking security seriously, services are configured in secure way and connection between internal servers and cloud services is secure. Different frameworks take cloud into consideration in different ways. For example, ISGcloud emphasizes on governance and analysis of cloud security, while QUIRC focuses on individual security objectives defined by the organization conducting risk assessment. In any case, it is important to make sure that data is secure in the cloud environment.

Second research question was about **how to implement risk assessment framework GBM-OA in practice?** GBM-OA consist of defining stakeholders of security risk analysis, definition of risk measurement criteria, identification of producers and users of information, identifying genres of communication, development of information asset profiles with genre properties, identification of containers and identification of risks and mitigation strategies. In this case study, the process was cut into three workshops to make sure that content would not be too heavy for the participants. Before the workshops, introductory sessions about the framework was held for the participants so they were able to familiarize with the framework before starting the work. During workshops, internal documentation was created represent producers and users of information, genres, containers, and risks. Time available for the workshops was limited, so focus had to be on few detailed risks in case of having multiple risks with little details. At the end, participants were satisfied with the results.

Third research question was about **how well GBM-OA suits to case context?** Qualitative semi-structured interviews were conducted to find answer to this question. According to the answers from the interviews, the framework does not suit to the context as it is. Steps of the framework should be integrated into development process. In addition, participants suggested a new step to the framework, where most important impact areas for the context would be defined to produce more value from the framework to the context. Right now, there is no instructions in the framework about iteration of the assessment, so it would be useful to consider how the framework should be iterated efficiently.

4.3 Implications for research and methodology development

In this study, it was clear that GBM-OA framework contains characteristics which are difficult to understand if the participants are not familiar with security risk assessment. During the assessment, participants with some experience from risk assessment did not have many difficulties, but participants with little experience with security risk assessment found it difficult to understand terminology and the steps used in the framework. Because of these difficulties, a lot of time was used in explaining what the terminology means and what the different steps are. When researchers are conducting a study about information security risk assessment frameworks, sufficient time should be granted for the participants to get familiar with the framework. This way the assessment will go through smoother, and the researcher can focus on making observations.

For method development, it is necessary to try the framework out in different organizations. Since the framework is a qualitative approach that relies on the expertise of the participants, it is also important to take note how different participants behave during the assessment. During this study, it was noted that some participants do not like strict processes, and filling predefined documentation is not efficient and valuable. At the same time, some participants felt that predefined documentation and strict processes make it easy to use the framework, since participants do not have to define things themselves and they can focus on the risk assessment. It is important to find a compromise between these two opinions to make the framework suitable to as many use cases as possible.

4.4 Implications for Practice

Discussions with the participants during the study revealed, that security related assessments are not so common in the team. Security is usually discussed on higher level than in daily work. Exception are infrastructure related topics, where security always needs to be discussed. It was also revealed that the participants were not very familiar with different ways of conducting information security risk assessment. The team should be more included in security related discussions to raise awareness about information security to the team to make sure, that every member of the team knows the state of security in the software. This way, the team can more easily contribute for the security and raise their own concerns about it.

For information security professionals, it can be noted that security is just one component in whole software development. Developers do not have all their time to focus on security, but they are required to focus on multiple different components. This is especially visible in DevOps culture. Therefore, there will always be some problems with security. Security professional should support individual developers by training them in context of security. In this study, participants were not sure about what are all possible vulnerabilities in the system, but they were sure that there are many. This shows that developers understand that there are vulnerabilities, but they do not know about them in detail. Security professionals can help developers by identifying the problems and teaching them how to avoid them. This way the developers can try and avoid creation of vulnerabilities.

5. Conclusions

In this thesis I have discussed about information security risk assessment in context of centralized CI/CD environment. Since organization utilize automation in their business, much of their confidential information is stored to databases and information systems. These information assets can be valuable targets for attackers, and loss of confidential information can have devastating consequences for companies. Hence, companies have to invest in information security solutions to protect their information assets.

Information security risk assessment is part of risk management, where you identify possible vulnerabilities against your assets which could be exploited by attackers and define countermeasures for those vulnerabilities. To help companies and organization to conduct successful information security risk assessment, multiple different frameworks has been developed. These frameworks can be divided to qualitative and quantitative approaches. Qualitative approaches focus on the people and they rely on the expertise and knowledge of participants. Quantitative frameworks focus on calculation of possible losses if risks realize, and the impact and severity of that risk is defined based on that estimation. Selection of suitable framework depends on the resources available for the assessment, expertise of staff and context of assessment target.

In this thesis I have evaluated genre-based risk assessment framework GBM-OA by conducting security risk assessment in practice. After the assessment, interviews were conducted with participants to find out how well the framework suited in the context. Advantages of the framework found by the participants were the definition of environment and the needed time from beginning to the end. Drawbacks of the framework were the confusing terminology used in the framework and repetition in filling the templates. The findings from the study show that the framework is not suitable for the context since usage of the framework would require separate assessment iteration. The participants found that risk assessment should be integrated to development cycle and it should not be separate process. Improvement ideas for the framework proposed by the participants were adding one step to the framework where impact areas are defined and adding instructions about iteration of the framework.

DevOps is rapidly evolving culture since companies are continuously trying to improve their software development towards automation and fast release cycles. This evolution might provide interesting aspects also towards security. This can already be seen from introduction of DevSecOps. Also, providers of the tools used in implementation of DevOps practices are trying to evolve. Current trend seems to be that the providers are trying to implement their own CI/CD pipelines (GitHub actions, JFrog pipelines). This trend will help companies and organizations in the future by decreasing the number of different tools required to implement DevOps practises. Unfortunately, this trend does not include security related features, so it will be interesting to see when these providers start to think about how important information security actually is.

5.1 Limitations

Since the target of this study was rather small team (less than 20 employees), it is difficult to conclude if the findings of this study would reflect similarly in bigger teams. Big teams have multiple engineers from different backgrounds and the variety of expertise could help with the selection of participants. In case of this study, only handful of people could be considered as possible participant. Hence there was not much variety between expertise of the participants. If there would be bigger pool of expertise to select from, results of the assessment might have been different.

The author of this thesis is not an expert on information security, and it was first time that the author was conducting information security risk assessment in practice. This might affect the results of this study. If the person responsible of conducting risk assessment has previous experience about different assessment frameworks, reflecting practicalities of GBM-OA and other frameworks could help when conducting risk assessment using GBM-OA.

People who would be participating in the risk assessment were selected in the beginning of the assessment process. Unfortunately, not all of the selected people were able to participate in the assessment. Hence there was a gap between planned about of expertise in the assessment and the actual amount of expertise. If all selected people would have been able to participate, results of this study might have changed.

5.2 Further research

This study was conducted in one team and the framework was run through once. To verify the findings from this study, additional studies should be conducted in different companies and in similar context. Also, running the framework through multiple times can produce different or new findings.

When talking about information security risk assessment in general, it is not fun or rewarding work for the participants. This was also seen in this study from discussions with the participants and from the way they behaved during the assessment. This is a problem, especially in qualitative frameworks, since risk assessment is based on participants expertise and experiences. Ways of how to motivate participants should be studied. In addition, it would be interesting to see how the motivation of participants affects the results in qualitative risk assessment frameworks.

The objective of this study was to find out how well GBM-OA would suit in context of centralized CI/CD environment. It would be interesting to see how well the framework would suit in the context compared to other qualitative frameworks. If company or organization would need to select a qualitative information security risk assessment framework in this context, it would be possible that the company or organization would select GBM-OA as risk assessment framework even though it would not be suitable if it would suit better than other options.

Findings from this study show that the major reason why GBM-OA is not suitable for the context is that the framework does not fit into DevOps practicalities. This finding might be different if the team would be using DevSecOps instead of DevOps. A study should be conducted in centralized CI/CD environment in DevSecOps way of thinking to see if the framework would suit in DevSecOps practicalities. In addition, ways of how to integrate GBM-OA into DevSecOps practicalities should be investigated.

References

Aagedal, J. O., Den Braber, F., Dimitrakos, T., Gran, B. A., Raptis, D., & Stolen, K. (2002, September). Model-based risk assessment to improve enterprise security. In Proceedings. Sixth International Enterprise Distributed Object Computing (pp. 51-62). IEEE.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. ICIS 2006 Proceedings, 94.

Agrawal, V. (2017). A Comparative Study on Information Security Risk Analysis Methods. JCP, 12(1), 57-67.

Agrawal, V., & Szekeres, A. (2017, June). CIRA Perspective on Risks Within UnRizkNow—A Case Study. In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 121-126). IEEE.

Alberts, C. J., & Dorofee, A. J. (2003). Managing information security risks: the OCTAVE approach. Addison-Wesley Professional.

Al-sa'eed, M. T. A., Al-mahamid, S. M., & Al-sayeed, R. M. (2012). The Impact of Control Objectives of Information and Related Technology (COBIT) Domain on Information Criteria and Information Technology Resources. Journal of Theoretical & Applied Information Technology, 45(1).

Aven, T. (2012). The risk concept—historical and recent development trends. Reliability Engineering & System Safety, 99, 33-44.

Baker, W. H., Rees, L. P., & Tippett, P. S. (2007). Necessary measures: metric-driven information security risk assessment and decision making. Communications of the ACM, 50(10), 101-106.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. ACM Computing Surveys (CSUR), 25(4), 375-414.

Baskerville, R., & Myers, M. D. (2004). Special issue on action research in information systems: Making IS research relevant to practice: Foreword. MIS quarterly, 329-335.

Beck, K. (1999). Embracing change with extreme programming. Computer, 32(10), 70-77.

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. NursingPlus Open, 2, 8-14.

Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In Proceedings of the 2001 workshop on New security paradigms (pp. 97-104).

Buecker, A., Lodewijkx, K., Moss, H., Skapinetz, K., & Waidner, M. (2009). Cloud security guidance ibm recommendations for the implementation of cloud security. IBM Corp, 2.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34(3), 523-548.

Davison, R. M., Martinsons, M. G., & Ou, C. X. (2012). The roles of theory in canonical action research. MIS Quarterly, 763-786.

Dhillon, G. (2007). Principles of information systems security: Texts and cases. John Wiley & Sons Incorporated.

Djemame, K., Armstrong, D., Kiran, M., & Jiang, M. (2011). A risk assessment framework and software toolkit for cloud service ecosystems. Cloud Computing, 119-126.

Dutta, M. (2019). [DevOps cycle] [Figure] Medium. https://medium.com/@mainakdutta76/before-and-after-of-devops-a-peek-into-agile-devops-3600c26129ac

Dybå, T., Sjøberg, D. I., & Cruzes, D. S. (2012, September). What works for whom, where, when, and why? On the role of context in empirical software engineering. In Proceedings of the ACM-IEEE international symposium on Empirical software engineering and measurement (pp. 19-28).

Dyer, J. S. (2005). MAUT—multiattribute utility theory. In Multiple criteria decision analysis: state of the art surveys (pp. 265-292). Springer, New York, NY.

de Gusmão, A. P. H., e Silva, L. C., Silva, M. M., Poleto, T., & Costa, A. P. C. S. (2016). Information security risk analysis model using fuzzy decision theory. International Journal of Information Management, 36(1), 25-34.

Ebert, C., Gallardo, G., Hernantes, J., & Serrano, N. (2016). DevOps. Ieee Software, 33(3), 94-100.

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security.

Fredriksen, R., Kristiansen, M., Gran, B. A., Stølen, K., Opperud, T. A., & Dimitrakos, T. (2002, September). The CORAS framework for a model-based risk management process. In International Conference on Computer Safety, Reliability, and Security (pp. 94-105). Springer, Berlin, Heidelberg.

Fruhwirth, C., & Mannisto, T. (2009, October). Improving CVSS-based vulnerability prioritization and response with context information. In 2009 3rd International Symposium on Empirical Software Engineering and Measurement (pp. 535-544). IEEE.

Gordon, L. A., & Loeb, M. P. (2006). Managing cybersecurity resources: a cost-benefit analysis (Vol. 1). New York: McGraw-Hill.

Halkidis, S. T., Tsantalis, N., Chatzigeorgiou, A., & Stephanides, G. (2008). Architectural risk analysis of software systems based on security patterns. IEEE Transactions on Dependable and Secure Computing, 5(3), 129-142.

Herzog, A., Shahmehri, N., & Duma, C. (2007). An ontology of information security. International Journal of Information Security and Privacy (IJISP), 1(4), 1-23.

Horton, J., Macve, R., & Struyven, G. (2004). Qualitative research: experiences in using semi-structured interviews. In The real life guide to accounting research (pp. 339-357). Elsevier.

Humble, J., & Farley, D. (2010). Continuous delivery: reliable software releases through build, test, and deployment automation. Pearson Education.

Jabbari, R., bin Ali, N., Petersen, K., & Tanveer, B. (2016, May). What is DevOps? A systematic mapping study on definitions and practices. In Proceedings of the Scientific Workshop Proceedings of XP2016 (pp. 1-11).

Jacobson, I., Booch, G., Rumbaugh, J., Rumbaugh, J., & Booch, G. (1999). The unified software development process (Vol. 1). Reading: Addison-wesley.

Joh, H., & Malaiya, Y. K. (2011, July). Defining and assessing quantitative security risk measures using vulnerability lifecycle and cvss metrics. In The 2011 international conference on security and management (sam) (pp. 10-16).

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. Journal of advanced nursing, 72(12), 2954-2965.

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. Computers & Security, 24(2), 147-159.

Karabacak, B., & Sogukpinar, I. (2006). A quantitative method for ISO 17799 gap analysis. Computers & security, 25(6), 413-419.

Khan, M. A. (2017). Efficacy of OCTAVE Risk Assessment Methodology in Information Systems Organizations. International Journal of Computer Applications Technology and Research, 6(6), 242-244.

Lam, T., Chaillan, N. (2019). [DevSecOps Software Lifecycle] [Figure]. The U.S. Department of Defense. https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583

Lee, K., Murray, D., Hughes, D., & Joosen, W. (2010, November). Extending sensor networks into the cloud using amazon web services. In 2010 IEEE International Conference on Networked Embedded Systems for Enterprise Applications (pp. 1-7). IEEE.

Lenkala, S. R., Shetty, S., & Xiong, K. (2013, May). Security risk assessment of cloud carrier. In 2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing (pp. 442-449). IEEE.

Liu, S., Kuhn, R., & Rossman, H. (2009). Understanding insecure IT: Practical risk assessment. IT professional, 11(3), 57-59.

Lwakatare, L. E., Kilamo, T., Karvonen, T., Sauvola, T., Heikkilä, V., Itkonen, J., ... & Lassenius, C. (2019). DevOps in practice: A multiple case study of five companies. Information and Software Technology, 114, 217-230.

Malaurent, J., & Avison, D. (2016). Reconciling global and local needs: a canonical action research project to deal with workarounds. Information Systems Journal, 26(3), 227-257.

Mao, R., Zhang, H., Dai, Q., Huang, H., Rong, G., Shen, H., ... & Lu, K. (2020, December). Preliminary Findings about DevSecOps from Grey Literature. In 2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS) (pp. 450-457). IEEE.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.".

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Mell, P., Scarfone, K., & Romanosky, S. (2007, June). A complete guide to the common vulnerability scoring system version 2.0. In Published by FIRST-forum of incident response and security teams (Vol. 1, p. 23).

Myler, E., & Broadbent, G. (2006). ISO 17799: Standard for security. Information Management, 40(6), 43.

Myrbakken, H., & Colomo-Palacios, R. (2017, October). DevSecOps: a multivocal literature review. In International Conference on Software Process Improvement and Capability Determination (pp. 17-29). Springer, Cham.

Olsson, C. M., & Henfridsson, O. (2005). Designing context-aware interaction: An action research study. In Designing ubiquitous information environments: Socio-technical issues and challenges (pp. 233-247). Springer, Boston, MA.

Padyab, A. M., Päivärinta, T., & Harnesk, D. (2014, January). Genre-based assessment of information and knowledge security risks. In 2014 47th Hawaii International Conference on System Sciences (pp. 3442-3451). IEEE.

Paivarinta, T., Halttunen, V., & Tyrvainen, P. (2001). A genre-based method for information systems planning. In Information modeling in the new millennium (pp. 70-93). IGI Global.

Peltier, T. R. (2005). Information security risk analysis. CRC press.

Pooley, R., & King, P. (1999). The unified modelling language and performance engineering. IEE Proceedings-Software, 146(1), 2-10.

Poolsappasit, N., Dewri, R., & Ray, I. (2011). Dynamic security risk management using bayesian attack graphs. IEEE Transactions on Dependable and Secure Computing, 9(1), 61-74.

Rajbhandari, L., & Snekkenes, E. (2013, July). Using the conflicting incentives risk analysis method. In IFIP International Information Security Conference (pp. 315-329). Springer, Berlin, Heidelberg.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. Information and Software Technology, 58, 44-57.

Riungu-Kalliosaari, L., Mäkinen, S., Lwakatare, L. E., Tiihonen, J., & Männistö, T. (2016, November). DevOps adoption benefits and challenges in practice: a case study. In International Conference on Product-Focused Software Process Improvement (pp. 590-597). Springer, Cham.

Saripalli, P., & Walters, B. (2010, July). Quirc: A quantitative impact and risk assessment framework for cloud security. In 2010 IEEE 3rd international conference on cloud computing (pp. 280-288). Ieee.

Schatzki, T. R. (2002). The site of the social: A philosophical account of the constitution of social life and change. Penn State Press.

Sendi, A. S., Jabbarifar, M., Shajari, M., & Dagenais, M. (2010, May). FEMRA: Fuzzy expert model for risk assessment. In 2010 Fifth International Conference on Internet Monitoring and Protection (pp. 48-53). IEEE.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & security, 57, 14-30.

Shedden, P., Ruighaver, A. B., & Ahmad, A. (2010). Risk Management Standards-The Perception of ease of use. Journal of Information System Security, 6(3).

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. Vine.

Stamatiou, Y. C., Skipenes, E., Henriksen, E., Stathiakis, N., Sikianakis, A., Charalambous, E., ... & Papadaki, K. (2003). The CORAS approach for model-based risk management applied to a telemedicine service. Proc. Medical Informatics Europe (MIE'2003).

Stolen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S. H., ... & Aagedal, J. O. (2002). Model-based risk assessment-the coras approach. In iTrust Workshop.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS quarterly, 441-469.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. Nist special publication, 800(30), 800-30.

Stuter, L. M. (1996). The Delphi Technique: What is it. Lynn's Educational and Research Network.

Susman, G. I., & Evered, R. D. (1978). An assessment of the scientific merits of action research. Administrative science quarterly, 582-603.

Sánchez-Gordón, M., & Colomo-Palacios, R. (2020, June). Security as Culture: A Systematic Literature Review of DevSecOps. In Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops (pp. 266-269).

Taubenberger, S., Jürjens, J., Yu, Y., & Nuseibeh, B. (2011, June). Problem analysis of traditional it-security risk assessment methods–an experience report from the insurance and auditing domain. In IFIP International Information Security Conference (pp. 259-270). Springer, Berlin, Heidelberg.

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting: An examination of the psychological situation and defences of a work group in relation to the social structure and technological content of the work system. Human relations, 4(1), 3-38.

Vorster, A., & Labuschagne, L. E. S. (2005, July). A framework for comparing different information security risk analysis methodologies. In Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries (pp. 95-103).

Wangen, G. (2015). Conflicting incentives risk analysis: A case study of the normative peer review process. Administrative Sciences, 5(3), 125-147.

Wangen, G. (2017). Information security risk assessment: a method comparison. Computer, 50(4), 52-61.

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. International Journal of Information Security, 17(6), 681-699.

Whitman, M. E., & Mattord, H. J. (2011). Principles of information security. Cengage Learning.

Wyld, D. C. (2009). Moving to the cloud: An introduction to cloud computing in government. IBM Center for the Business of Government.

Xie, C., Anumba, C. J., Lee, T. R., Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). Supply Chain Management: An International Journal.

Zhang, S., Caragea, D., & Ou, X. (2011, August). An empirical study on using the national vulnerability database to predict software vulnerabilities. In International conference on database and expert systems applications (pp. 217-231). Springer, Berlin, Heidelberg.

Appendix A. Notes from risk assessment sessions

Session 1, PUI Matrix and Genre List

- Session started after long meeting, so participants were a bit tired.
- PUI matrix was easy to understand and we did not get stuck while defining producers and users.
- Definition of Genre List raised good discussion from both producer and user point of view, which helped us to get insight about details of each genre.
- Lack of details about the future caused problems while filling Genre List.
- Four producers and users of information found.
- 13 different genres found.

Session 2, Information containers

- Participants were already aware about what we will be doing during the session, so we got started quickly.
- Value of information containers was questioned. Participants did not understand how information containers would help us later with information risk definition.
- Participants did not understand the details of information containers, so a quick recap to introduction session was needed before moving on.
- First few containers took time before we were able to fill them, but afterwards the participants started to understand how the containers work and the definition started to move on quickly.
- Participants were able to define information container for each genre before time was up, so quick preview about session 3 was held.

Session 3, Information asset worksheets

- Session started later than planned due a long meeting before the session.
- Information asset worksheet proved hard to understand, so participants got stuck at some parts of the worksheet template.
- Definition of one risk took long time. It is possible that the three sessions were held to separately and the participants forgot what was previously defined.
- Since risks took long time to be defined, given time was not enough to fill the last asset worksheet. Last worksheet was filled by participants sending email to assessor.
- 4 asset worksheets filled.

Appendix B. Interview questions

1. After the introduction of the assessment framework, what was you feeling of the framework?
2. At the beginning of the assessment framework, what was your feeling about how the framework will go through?
3. After the assessment what was your feeling about the framework?
4. What do you think about the results?
5. How well you think the framework suits to the context?
6. What was the best part of the framework?
7. What was the worst part of the framework?
8. What do you think about the templates?
9. What would you change in the framework?
10. Were the people selected the right people?
11. Would you use this framework in another context?